VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

PENETRAČNÍ TESTOVÁNÍ ANC

PENETRATION TESTING OF ANC

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Jakub Dušek

AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák

SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Jakub Dušek**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2020/21

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Penetrační testování ANC

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je vyhodnocení bezpečnostního řešení, které nedávno začala využívat britská společnost pronajímající kancelářské prostory. Tento validační systém je založen na databázi MAC adres, databázi klientů a aktivním filtrování připojených zařízení. Prostředkem pro vyhodnocení bezpečnostního řešení je měření na základě hypotéz, podle kterých budou navržena bezpečnostní opatření pro vyřešení těchto problémů.

Základní literární prameny:

DONAHUE, G. A. Kompletní průvodce síťového experta. 1. vyd. Brno: Computer Press, 2009. ISBN 978-80-251-2247-1.

JORDÁN, V. a V. ONDRÁK. Infrastruktura komunikačních systémů I: univerzální kabelážní systémy. 2. vyd. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5115-5.

KUROSE, J. , K. ROSS a J. JONÁK. Počítačové sítě. 1. vyd. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

ONDRÁK, V. Počítačové sítě. Brno: VUT v Brně, Fakulta podnikatelská, 2014.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

Mgr. Veronika Novotná, Ph.D. ředitel	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Tato diplomová práce se zabývá vyhodnocením bezpečnostního řešení, které nedávno začala využívat britská společnost pronajímající kancelářské prostory. Tento validační systém je založen na databázi MAC adres, databázi klientů a aktivním filtrování připojených zařízení. V první části práce jsou vysvětleny pojmy počítačová síť, VLAN a základní pojmy potřebné pro porozumění funkce dynamického přiřazování VLAN a IP adres. Druhá část se věnuje měření na základě hypotéz, podle kterých jsou v poslední části navrhnuty opatření pro vyřešení těchto problémů.

Abstract

This diploma thesis deals with the evaluation of a security solution that was recently deployed by a British company renting office space. This validation system is based on a database of MAC addresses, a database of clients and active filtering of connected devices. The first part explains the concepts of computer network, VLAN and basic concepts needed to understand the function of dynamic assignment of VLAN and IP addresses. The second part is devoted to measurements based on hypotheses, according to which measures are proposed in the last part to solve these security problems.

Klíčové slova

Počítačová sít, Ethernet, TCP/IP, VLAN, síťová bezpečnost, MAC adresa, ARP, spoofing

Key words

Computer network, Ethernet, TCP/IP, VLAN, network security, MAC address, ARP, spoofing

Bibliografická citace

DUŠEK, Jakub. *Penetrační testování ANC* [online]. Brno, 2021 [cit. 2021-04-14]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/134348. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Tišnově dne 15. května 2021

……

podpis studenta

Poděkování

Především bych chtěl poděkovat vedoucímu své bakalářské práce panu Ing. Petrovi Sedlákovi a oponentovi Ing. Jakubovi Přibylovi za odbornou konzultaci a výpomoc v průběhu psaní práce. Dále pak panu Ing. Martinovi Křivému za poskytnutí prostředků a odborné výpomoci z jeho společnosti.

Obsah

Úvod

Tato diplomová práce se bude věnovat ověření bezpečnosti systému, který pro svoji síť aplikoval klient společnosti Dworkin spol. s r.o., pomocí penetračního testování. Tato společnost bude zároveň poskytovat prostředky, zařízení a znalosti pro uskutečnění praktické části diplomové práce.

Před začátkem práce bylo potřeba vytyčit cíle a hypotézy, které jsou postupně v celé práci rozpracovány, později aplikovány a po naměření výsledků budou vyhodnoceny. Následně z těchto měření budou vyvozeny důsledky pro společnost a navržena opatření, která mají mít za úkol eliminovat tyto problémy a ochránit společnost před finančními následky. Důvod pro tohle testování je využívání sdílené serverovny a infrastruktury pro více klientů. Pro lepší představu se jedná o jednu masívní síť využívající sdílený hardware, který je síťově rozdělen na sekce, které mezi sebou nemůžou logicky komunikovat.

První část práce je věnována popisu pojmů, které jsou pro pochopení práce nezbytné. Tato teoretická východiska mají pomoci se správnou interpretací této práce. Jsou v ní vysvětleny obecně důležité technické termíny jako počítačová síť, MAC adresy, bezpečnost počítačových sítí atd., které by měla obsahovat každá práce zaměřená na bezpečnost informačních systémů.

V další části je obsažena analýza současného stavu. Je zde představena společnost Dworkin spol. s r.o. a testovací prostředí, které tato společnost poskytla. Dále je tu vypracována analýza systému doprovázejícího technologii přiřazování VLAN. Dále představuje metodiku testování jednotlivých hypotéz, samotné jejich testování a interpretaci výsledků, které z testování vyšly. Také obsahuje fotodokumentaci hardwaru, který byl využit pro sestavení testovacího centra ve všech svých konfiguracích, jeho popis a vysvětlení účelu v testování. Práce pokračuje vysvětlením a popisem, jakým způsobem technologie ANC funguje v případě této sítě a jak je u společnosti implementována. V poslední kapitole je zpracována analýza finančních rizik plynoucích z případných trhlin, které se při testování mohou objevit.

Poslední část se zabývá návrhy, které mají za úkol vyřešit bezpečnostní problémy, které byly během analytické části nalezeny. Věnuje se také interpretaci analýzy finančních rizik z předchozí části. Na konci je obsaženo ekonomické zhodnocení, které zahrnuje teoretické ekonomické dopady úniku dat jak klientů, tak samotné společnosti. V tomto ekonomickém zhodnocení jsou obsaženy i náklady na vyřešení nalezených problémů.

Vymezení problémů a cíle práce

Tato diplomová práce se zabývá vyhodnocením bezpečnostního řešení, které nedávno začala využívat britská společnost pronajímající kancelářské prostory. Tento validační systém je založen na databázi MAC adres, databázi klientů a aktivním filtrování připojených zařízení. Všechno testování bude probíhat z pozice nasazeného technika, který je zaměstnaný ve firmě poskytující veškerou podporu z hlediska IT pro tuto společnost.

Díky zkušenostem získaných při stovkách instalací pro tohoto klienta bylo možné se dostat do blízkého kontaktu s tímto systémem. Při těchto instalacích nastalo několik možných scénářů, pomoci kterých by mohlo dojít k napadnutí sítě. Hlavním předpokladem pro úspěšné vypracování této diplomové práce je zachovat informační bezpečnost pro všechny zainteresované strany. Z tohoto důvodu všechny testy a měření probíhají v laboratorních podmínkách, na kterých se shodly obě zainteresované strany. Nutné je ovšem poznamenat, že podmínky odpovídají reálnému provozu a nijak neovlivňují naměřené výsledky. Tyto podmínky představuje testovací centrum, které je postavené v logistickém centru společnosti Dworkin spol. s r.o. v Brně.

Hypotézy pro měření a vyhodnocení:

- **První hypotézou** pro výskyt bezpečnostní trhliny je zastaralý hardware centra. Jelikož klient provozuje tento systém na poměrně širokém spektru modelů přepínačů, několika typech firewallů, a navíc na několika tisících centrech, často se stane, že z důvodu finanční a časové náročnosti nejsou všechny sítě vybaveny nejnovějším standardem hardwaru a softwaru. Situace, kdy se na centru objevuje zastaralý systém je poměrně častá, jelikož existuje velké množství center, která byla otevřena i více než před dvaceti lety a při jejich otevření ještě neexistoval hardware, který tuto technologii podporoval. Zařízení jsou samozřejmě postupně vyměňována za podporovaná, ale vzhledem k obrovskému množství center, a ještě většímu množství hardware je to pomalý proces. Tato funkcionalita funguje nejlépe na přepínačích Cisco řady Catalyst 2960 a nově nastupující řadou Catalyst 9200. V případě, kdy síť obsahuje některý ze starších modelů (Catalyst 3560, Catalyst 3570 atd.) může být funkcionalita omezena. Je zde několik důvodů,

např. nižší výpočetní výkon, menší operační nebo vyrovnávací paměť, atd. V těchto případech se může stát, že nastanou chyby nebo konflikty a VLANy nejsou přiřazeny správně nebo vůbec. Tato hypotéza bude problém podrobně zkoumat a zjišťovat, jestli představuje bezpečnostní problém pro tuto společnost.

- **Druhá hypotéza** bude zkoumat, jak se síť chová v případě, kdy se útočník se svým zařízením pokusí vydávat za již existující zařízení, které je již registrované pod existujícím klientem s přiřazenou virtuální sítí. Tato možnost počítá s fyzickým přístupem k zařízení, a to z důvodu nutnosti znalosti MAC adresy zařízení. Získání adresy bude zajištěno pomocí přenosného směrovače nebo přečteno přímo ze zařízení (typicky stolní PC, Wi-Fi AP, tiskárna). S útokem na virtuální síť vybraného klienta se začne v momentě, kdy budou známy všechny potřebné údaje.
- **Třetí hypotéza** počítá s pozitivním výsledkem druhé hypotézy, jelikož je nutné být ve stejné virtuální síti jako ostatní klientská zařízení. V případě, že by druhá hypotéza nevyšla, je možnost na testovacím centru laboratorně vytvořit podmínky shodné s reálným prostředím. Obsahem této hypotézy bude aktivní odposlech sítě (ARP spoofing, ARP poisoning). Cílem je zjistit, zdali je možné pomocí těchto technik dosáhnout výsledku. Představa úspěšného výsledku je útok Man in The Middle na určité zařízení s možností odposlechu provozu napadeného zařízení. Jelikož není známá úroveň zabezpečení a ochrana počítačové sítě, předpokládá se, že není žádná. V případě, že by byl útok úspěšný, jednalo by se o vážnou bezpečnostní chybu v ochraně počítačové sítě.

Cílem práce je nalézt bezpečnostní trhliny při přiřazování VLAN a IP adres, navrhnout změny systému, které by dokázaly těmto problémům zabránit. Je důležité zmínit, že se práce nezabývá sociálním inženýrstvím ani zabezpečením databází MAC adres a uživatelů systém využívajících. Jedná se čistě o zabezpečení systému jako takového. Dále je cílem zhodnotit finanční náročnost případných náprav nalezených problémů. Data ohledně cen zařízení, cena jejich instalace a případného počtu ohrožených center, kterých se tyto problémy mohou týkat jsou známé z databáze systémů, které jsou napojeny na služby společnosti Dworkin spol. s r.o.

1 Teoretická východiska práce

Teoretická část této diplomové práce se zabývá vysvětlením pojmů a principů, které je nutné znát pro správné pochopení jejího zaměření Tyto pojmy jsou např. vysvětlení co jsou počítačové sítě a jak je dělíme, dále jsou vysvětlené pojmy související se zabezpečením, bezpečnostními hrozbami a je zde vysvětleno pár základních typů útoku, které jsou využívány pro napadnutí sítí.

1.1 Počítačová síť

Tento pojem označuje dvě a více vzájemně propojených zařízení (např. počítače, servery, tiskárny atd.), které si mezi sebou vyměňují informace. Tyto informace jsou sdíleny za pomoci daného protokolu, který se může lišit v závislosti na užití a změření sítě (1).

Počítačová síť se skládá z komunikační infrastruktury a koncových uzlů. Komunikační infrastruktura zahrnuje pasivní vrstvu a aktivní prvky. Pasivní vrstva obsahuje kabeláž, konektory, zásuvky, rozvaděče, kabelové trasy a v případě bezdrátových sítí i prostor, ve kterém jsou data přenášena. Mezi aktivní prvky patří všechna zařízení, která data přijímají, zpracovávají a poskytují dále v rámci sítě. Jsou to například přepínače, směrovače, rozbočovače, firewally apod. (2).

1.1.1 Rozdělení sítí podle rozsahu

Rozsah sítě je možno rozdělit do několika kategorií podle jejich rozsahu. Od nejmenší rozlohy jsou řazeny následovně: PAN, LAN, MAN, WAN (2).

- Personal Area Network (PAN) se dá přiblížit jako osobní síť, která je tvořená pouze zařízeními jedné osoby, jako jsou mobilní telefony, notebooky, tablety a v současné době i různé senzory a prvky chytrých domácností. Zahrnuje pouze zařízení, které jsou v přímém dosahu této osoby a tím je její rozsah pouze v rámci jednotek metrů. Používá se pro vzájemnou komunikaci mezi zařízeními nebo k připojení k okolním sítím. Způsoby přenosu dat v této síti může být jak drátový (např. USB) tak stále častěji bezdrátový (např. IrDA, Bluetooth, Wi-Fi) (2).

- Local Area Network (LAN) má větší rozsah a většinou se vztahuje na celý objekt nebo jeho část (podlaží, oddělení, místnost). Vyznačuje se vysokými přenosovými rychlostmi až v řádech Gbit/s. Nejčastější technologie využívané pro přenos signálu jsou Ethernet a Wi-Fi (3).
- Metropolitan Area Network (MAN) je rozlehlá počítačová síť, která je poskládána z několika menších celků, které mohou být ve své rozloze velké jako budovy, jejich části nebo až bloky měst. Jednotlivé bloky sítí jsou většinou propojeny pomocí směrové Wi-Fi nebo optického nebo metalického kabelu. Metropolitní síť je optimalizovaná pro co největší rozsah a dostupnost (3).
- Wide Area Network (WAN) se využívá pro spojování jednotlivých sítí typu LAN nebo MAN. Zaručuje, aby uživatelé a počítače v různých takto propojených sítích mohli komunikovat mezi sebou. Jednotlivé uzly se nachází daleko od sebe v různých městech nebo krajích a v některých případech i kontinentech. Propojení jednotlivých uzlů je realizováno pomocí propojovacích linek, které mohou být soukromé, ale většinou se jedná o pronajaté úseky. Tyto linky jsou zpravidla tvořeny optickými kabely. Nejznámější a nejrozšířenější síť typu WAN je internet (3).

1.1.2 Základní aktivní prvky počítačových sítí

Tato kapitola se zabývá vysvětlením a představením jednotlivých aktivních prvků, které jsou v této práci zmiňovány nebo používány při reálném testování. Při reálném využití se prvky mohou lišit nebo jsou například slučovány a provozovány z jednoho zařízení pro snížení nákladů a zvýšení spolehlivosti.

- **Směrovač (router)** je zařízení, které má za úkol směřovat (routovat) provoz mezi dvěma sítěmi, a to sítěmi WAN (vnější) a LAN (vnitřní). Tyto sítě mohou fungovat na stejné technologii TCP/IP nebo na různých technologiích např. DSL. Router je zařízení, které je vstupní bránou z vnějšího internetu do vnitřní sítě (1).
- **Firewall** slouží jako filtr, jehož funkce je třídit příchozí a odchozí komunikaci. Jeho úkolem je sledovat procházející komunikaci a na základě daných pravidel rozhodovat, co je do sítě vpuštěno a co je z ní vypuštěno. Díky jeho povaze je ho možné provozovat jako fyzické zařízení či případně jako službu. Rozdíl mezi těmito způsoby je cena a výkon. Pro menší sítě, kde je hleděno především na cenu

zařízení se často využívá jeho softwarová verze, která běží např. na serveru. Nevýhodou tohoto řešení je nižší výkon způsobený využíváním hardware, který není pro tento úkol vyloženě vyvinutý. V případě opačném, kdy jde o fyzické zařízení, se zvyšuje cena, ale zároveň i propustnost a výkon. Navíc je zde menší prostor pro bezpečnostní trhlinu, protože se jedná o čistě účelově vyrobené zařízení se softwarem a firmwarem vytvořeným přímo na míru. Je to další zařízení, které dokáže plnit podobnou funkci jako router a oddělovat sítě (1).

- **Přepínač** je zařízení, které velmi jednoduše vzato slouží jako replikátor portů. Je to funkce, kterou opravdu vykonává ve své úplně nejzákladnější konfiguraci. Pokud se jedná o přepínač, který je spravovaný, nastupuje i logika aktivně ovlivňující provoz, který prochází skrz něj (2).
- **Rozbočovač** je z hlediska vzhledu podobné zařízení jako přepínač, s rozdílem chybějící vnitřní logiky. V případě, že se jedná o rozbočovač je provoz skrz něj procházející rozesílán na všechny jeho porty. Z tohoto důvodu je jeho využívání méně bezpečné a účinné (4).
- **Server** je obecné označení pro počítač, který poskytuje nějaké služby. Jsou zde ovšem další charakteristiky, které závisí na jeho užití. Objevují se zde možnosti pro redundantní užití jednotlivých prvků jako jsou zdroje elektrické energie nebo pevné disky. Dále se tu uplatňuje technologie hot swap což je možnost výměny prvku za běžného provozu (4).
- **Přístupový bod** je síťové zařízení poskytující bezdrátové připojení pomocí technologie Wi-Fi do vnitřní sítě. Takto připojená zařízení se chovají stejně jako zařízení připojená kabelem a díky tomu na nich fungují stejné služby. Menšími nevýhodami jsou delší odezva a snížená rychlost nebo občasná nestabilita připojení, která může být ovlivněna počasím, zdmi, počty okolních klientů apod. (2).

1.1.3 Automatická síťová konfigurace (ANC)

Technologie ANC je v reálném prostředí využívána pro automatizaci rutinních akcí, které nevyžadují vstup z vnější pro dokončení. Úkony vhodné pro tuto technologii jsou:

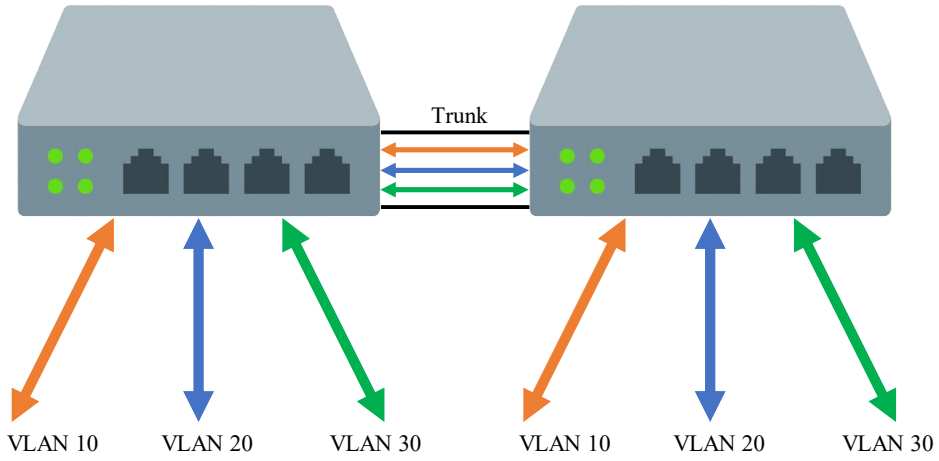
- Zálohování síťové konfigurace v automatickém režimu je jasně nadefinováno a většinou funguje formou zkopírování kompletní konfigurace každého síťového zařízení na přiřazené zařízení (typicky NAS). Jelikož je velikost konfiguračních souborů většinou v desítkách kilobajtů je možné v úložišti uschována celá historie konfigurací. Díky tomu je možné v případě zjištěné chyby vysledovat, kdy chyba vznikla a kdo ji vytvořil. Navíc je možné v případě nestandartního chování sítě obnovit konfiguraci do fungující ho stavu.
- Kontrola aktuálnosti softwaru síťových zařízení je z pravidla provázána s úložištěm, na kterém jsou uloženy bitové kopie firmwarů. Všechny verze, které jsou do úložiště přidány jsou již otestovány a schváleny pro fungování v daném prostředí. Díky tomu je následná distribuce aktualizací rychlá a efektivní. Z pravidla probíhá mimo pracovní dobu poté co je vytvořena záloha síťové konfigurace.
- Automatické nastavení nových zařízení při rozšiřování sítě je již značně pokročilá technika používaná pro sítě, které vyžadují co nejkratší výpadky během údržby. Většinou se nejedná o konfiguraci dalších přidávaných zařízení, ale o načtení již existující konfigurace ze zálohy a aktualizaci jeho softwaru na požadovanou verzi při jeho výměně.
- Automatická konfigurace portů na přepínači je forma ANC, o kterou se zajímá tato diplomová práce. Jejím úkolem je měnit konfigurace jednotlivých portech přepínače v reálném čase podle toho jaká jsou k nim připojena zařízení. Pro rozhodování o tom, jaká konfigurace je portu zaslána jsou využívány různé logiky rozpoznávání zařízení. Nejjednodušší způsob rozpoznání zařízení je podle jeho MAC adresy nebo v případě, kdy má nastavenou statickou IP adresu, tak podle ní.

Všechny tyto úkoly jsou nastaveny podle pevně dané logiky a jsou vytvořeny tak aby šetřili práci šítovým inženýrům, další výhodou je vyhýbání se chybám, které mohou při manuální práci s konfiguracemi nastat (5).

1.1.4 Management portů na přepínači

Jednotlivé porty na přepínačích mohou mít různé nastavení podle funkce, kterou vykonávají. V této kapitole jsou vysvětleny pouze ty základní, které jsou důležité pro tuto práci.

- **Access port** je výchozí nastavení portu na přepínači. V tomto nastavení je mu přiřazena VLAN 1. Poté už je na uživateli, do jaké VLAN port zařadí. Pro jeden port může být přiřazena pouze jedna VLAN, ve speciálních případech jich ovšem může být i více (6).
- **Trunk port** slouží pro propojení zařízení, která musí komunikovat ve větším počtu VLAN. Tyto zařízenou jsou např. přepínače, servery nebo přístupové body. Důvod, proč je tahle konfigurace vhodná pro komunikaci mezi zařízeními spočívá v tom, že zařízení přijme komunikaci z několika virtuálních sítí a podle toho je označí tagy. Díky těmto tagům je jasné, ze které sítě přišly a je možné s nimi dále pracovat a třídit je (6).



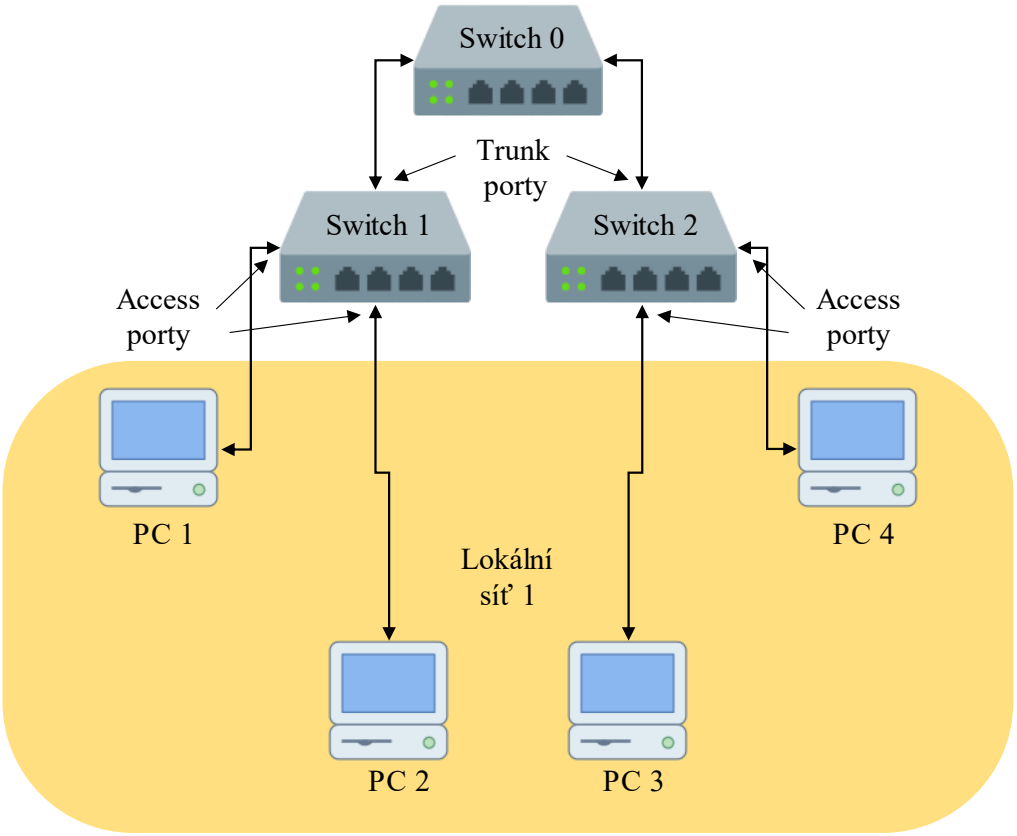
Obrázek 1: Princip trunk portu (4).

- **VLAN Trunk Protokol (zkráceně VTP)** slouží k redistribuci nakonfigurovaných VLAN z řídícího přepínače v síti, jinak by byla vyžadována ruční konfigurace VLAN databáze do každého přepínače v síti.
    - VTP server je nakonfigurován na řídícím přepínači, který spravuje a udržuje všechny virtuální LAN sítě, které jsou na síti nastaveny. Další funkcí, kterou má VTP server za úkol je distribuovat databázi VLAN do všech ostatních přepínačů v síti.
    - VTP klient přebírá poskytovanou databázi VLAN, která je mu poskytování od VTP serveru.

- VTP transparent přepínače jsou poslední možností nastavení VTP. Přepínače s tímto nastavením se neúčastní distribuce VLAN a pouze je poskytují dále. Není možné na nich nastavit virtuální LAN synchronizací databáze z řídícího přepínače (7).

1.1.5 Fyzické lokální počítačové sítě

Fyzická lokální počítačová síť je většinou síť rozsahu LAN, která je situovaná na jednom, ale může být i více přepínačích. Většinou se jedná o jednodušší sítě bez nebo s omezenou možností správy. Není to vhodná síť pro nasazení na veřejných místech nebo místech, která vyžadují vyšší standardy zabezpečení. Nejčastější užití jsou malé korporátní sítě nebo domácí sítě (1).

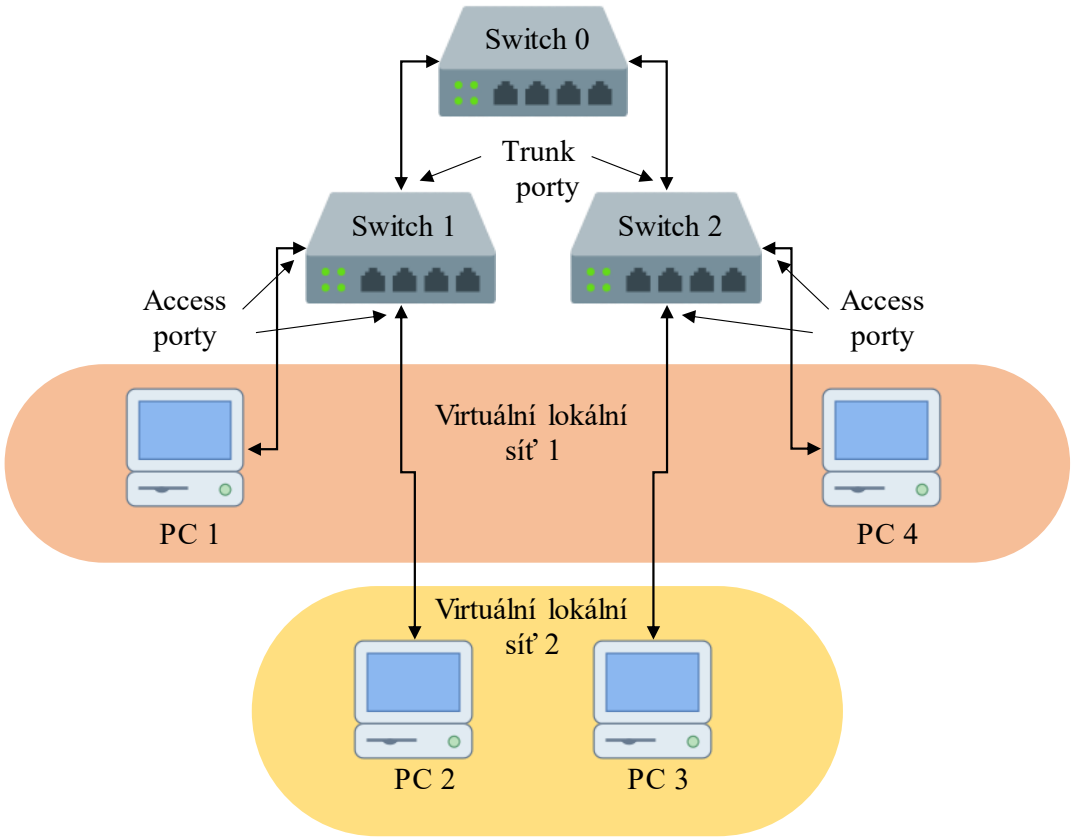


Obrázek 2: Diagram fyzické lokální sítě (3).

1.1.6 Virtuální lokální počítačové sítě

Virtuální LAN (zkráceně VLAN) rozdělují síť z logického pohledu nezávisle na jejím logickém uspořádání (ilustrováno na obrázku 3). Za pomoci VLAN zle dosáhnout stejného výsledku, jako kdybychom postavili libovolný počet (limitováno počtem VLAN, které je schopen zpracovávat přepínač) fyzicky oddělených sítí. Tyto sítě nejsou schopny spolu komunikovat a mají každá svůj IP rozsah. Jde o dělení sítě už na 2. vrstvě ISO/OSI modelu (8).

Pro použití v praxi je ovšem nutné mezi sítěmi komunikovat. Jelikož se VLAN logicky chová jako běžná síť, můžeme tedy mezi nimi použít jakýkoliv způsob směrování. Jsou tu i další možnosti, kdy dvě oddělené sítě vyžadují připojení do stejného zařízení – typicky např. servery. Řešení těchto situací je možné vyřešit zařazením zařízení do dvou VLAN (8).



Obrázek 3: Virtuální lokální počítačové sítě (3).

1.1.6.1 Přiřazování podle portů

Dělení zařízení do jednotlivých virtuálních sítí je prováděno staticky a je navázáno na jednotlivá čísla portů. Virtuální sítě zle přiřazovat jednotlivým zařízením i napříč několika propojených přepínačů, jak můžeme vidět na obrázku číslo 3. Také díky jejich propojení pomocí trunk portu. PC1 a PC4 jsou obě přiřazeny do virtuální sítě 1. PC2 a PC3 jsou obě přiřazeny do virtuální sítě 2 (4).

Jednotlivé porty jsou napevno nastaveny na statické nastavení. Neprobíhá na nich ověřování, jaké zařízení se připojuje. Pokud je do portu připojen další přepínač, je všem zařízením do něj připojených přiřazena stejná virtuální síť. Je to v současné době asi nejvíce používaná možnost. Můžeme to brát jako jednoduché a efektivní řešení, jelikož po připojení nového zařízení není nutné procházet žádnou složitou logikou a je mu přímo přiřazena virtuální síť a IP adresa (8).

Pro zlepšení bezpečnosti v případech, kdy se využívají sdílené serverovny, se dá přiřadit ke každému portu virtuální síť a MAC adresa zařízení, které je pro tento port určeno. Přístup k internetu je odepřen takovým zařízením připojených do portu na přepínači, která ale nejsou přiřazená k virtuální síti. Nejedná se ovšem o aktivní skenování a přiřazování virtuální sítě podle MAC adresy. Jedná se o čistě statické nastavení s možností filtrování, které přispívá ke zvýšení bezpečnosti sítě a větší kontrole. Nevýhodou tohoto řešení, je vyšší náročnost nastavení a nutnost zasahovat do konfigurace pokaždé, když je zařízení vyměněno za jiné (8).

1.1.6.2 Přiřazování VLAN podle MAC adres

Pro tento způsob přiřazování virtuálních sítí se využívají dva přístupy. Oba systémy dosahují výsledku jiným způsobem a jsou mířeny na jiné užití (4).

První způsob pracuje s databází MAC zařízení, která jsou uložena do VTP serveru. Porty nemají nastavenu žádnou virtuální síť a pracují s jinou technikou. Tato technika skenuje všechny rámce, které prochází při komunikaci sítí a podle tagů, které je rozesílá přímo na příslušné zařízení. Tato technika má několik nevýhod. První z nich je potřeba poměrně vysokého výkonu, jehož nedostatek v případě velkého vytížení sítě může zpožďovat doručování rámců a způsobovat tím zvýšení odezvy. Dalším problémem je

prostor pro generování chyb. Jelikož jsou všechny rámce směrovány po jejich přečtení může se stát, že při čtení nastane chyba a rámec je odeslán špatnému zařízení (3).

Druhá možnost, která je využívána pro přiřazování VLAN také spoléhá na databázi VLAN, pod kterou jsou přiřazeny jednotlivá zařízení. Jednotlivé porty v případě, kdy k nim není nic připojeno stejně jako v předchozím případě nemají žádnou konfiguraci. Po připojení zařízení je přečtena jeho MAC adresa a ta je vyhledána v databázi. Pokud je zařízení zařazeno pod VLANu, je k portu odeslána příslušná konfigurace. Výhodou tohoto nastavení je vysoká stabilita a rychlost po připojení zařízení a jeho přiřazení do správné virtuální sítě. Tohle přiřazení v případě, kdy je vše správně nastaveno probíhá okamžitě a nadále se port chová jako staticky nastavený. Tento systém je často využíván pro větší společnosti udržující databázi zařízení s MAC adresami a příslušnými virtuálními sítěmi centralizovaně. Při výpadku internetu u serveru, jež databázi drží, není možné nová zařízení správně řadit do virtuálních sítí, což je jeho nevýhodou (3).

1.1.7 Přiřazování IP adres v síti (DHCP)

Dynamic Host Configuration Protocol je protokol aplikační vrstvy z modelu TCP/IP, který se používá pro automatickou konfiguraci síťových parametrů pro zařízení připojovaných do počítačové sítě. Tímto mechanismem se výrazně ulehčuje práce síťových správců, jelikož připojené klienty automaticky informuje o parametrech, které jsou nutné pro správnou komunikaci pomocí IP protokolu. V tomto případě odpadá nutnost do procesu zasahovat a nastavovat každého klienta manuálně. Klientské zařízení tedy nemusí znát žádné informace o síti, ty jsou mu po zapojení automaticky poskytnuty. Konfigurace je klientům přiřazena na určitou dobu. Po uplynutí poloviny této doby si klient opětovně žádá o konfiguraci a ta je mu obnovena. V závislosti na počtu zařízení a obsazenosti rozsahu, který je pro DHCP přiřazen, se může konfigurace při přepojení zařízení změnit. Z důvodu této vlastnosti není nikdy jisté, jestli bude mít stanice stejnou IP i po přepojení, což v případě serverů, NASů nebo tiskáren není vhodné. Pro tyto případy je možné IP adresu z DHCP rozsahu vyjmout, přiřadit ji konkrétnímu zařízení (podle MAC adresy) a nastavit mu všechny parametry manuálně. Ty se mohou i lišit od parametrů ostatních stanic v síti (9).

Díky tomuto systému je významným způsobem zjednodušena správa sítě. Navíc ji centralizuje a umožňuje hromadnou změnu parametrů pro nové a stávající připojené stanice. Pomocí DHCP se nejčastěji nastavují tyto parametry sítě:

- IP adresa,
- maska sítě,
- výchozí brána,
- seznam dostupných DNS serverů,
- a další údaje jako NTP, WINS atd (9).

1.1.7.1 Dynamická alokace

V případě dynamické alokace DHCP server přiděluje IP adresy, které jsou nepoužívané v přiděleném rozsahu. Adresy jsou přiděleny na omezenou dobu, tím dovoluje po odpojení zařízení přidělit tuto adresu nové stanici. Tato funkce se využívá v případě, kdy existuje síť, do které se připojuje větší množství zařízení, než má přiděleno adres. Omezením tohoto způsobu je možnost přiřadit pouze tolik zařízení, kolik je v IP rozsahu adres. Z toho důvodu se počítá, že počty klientů se mění v průběhu používání a nikdy tuto hranici nepřekročí. Dále také nevadí neustálé změny adres jednotlivých zařízení (9).

Průběhu přiřazování konfigurace pomocí protokolu DHCP mohou být zapojeny 3 typy zařízení:

- **Server** udržuje a spravuje konfiguraci, která je nastavena správci sítě. Tento server může být nastaven na počítači, routeru, firewallu atd. Jeho úkolem je odpovídat na žádosti DHCP klientů a poskytovat jim přednastavené konfigurační parametry sítě.
- **Relay agent** je využíván v situaci, kdy existují dvě sítě nebo více sítí, ale DHCP server se nachází pouze v jedné z nic. V takovém případě nastaví správce sítě relay agenta na řídících přepínačích jednotlivých sítí. Pokud je agent nastaven správně, bude všechny DHCP dotazy přijaté ze sítě bez DHCP serveru přeposílat na DHCP server. Pro správnou identifikaci přidává agent ke každému dotazu číslo sítě a její masku. Díky tomuto označení je serveru známa zdrojová síť, ze které

dotaz přišel a je do ní následně i odeslána odpověď s příslušnou konfigurací. Relay agent tuto odpověď již nijak neovlivňuje pouze ji předá klientovi (9).

- **Klient** je každé jiné zařízení, které je do sítě připojeno a žádá o konfigurační parametry. Jsou to např. počítače, telefony, tablety atd. Po přiřazení těchto parametrů je mu oznámeno na jak dlouho mu jsou přiřazeny a po uplynutí této doby si zažádá o nové (9).

1.1.7.2 Statická alokace

V případě statické alokace je DHCP nakonfigurován tak, aby klientům přiděloval vždy stejnou IP adresu, která je navázána na MAC adresu zařízení. Pro správné fungování této funkce musí být vytvořena databáze, která obsahuje MAC adresy s příslušnými IP adresami. Tohle řešení znamená nemožnost změny IP adresy, po vypršení poloviny časového limitu si zařízení žádá o obnovení konfigurace. Odpověď na tento dotaz zní, že má zařízení přiřazenu statickou adresu. V případě, kdy je zařízení úplně odpojeno od sítě je možné, že bude adresa změněna a přiřazena jinému zařízení, jelikož není vyjmuta z rozsahu DHCP (9).

1.1.7.3 Manuální alokace

Pro manuální přiřazení IP adresy se nevyužívá DHCP serveru. Konfigurace je do zařízení nastavena ručně a není možné ji změnit na dálku. Využití této techniky je pro zařízení, u kterých je nutné, aby se jim i v případě odpojení nebo restartu sítě nezměnila IP adresa. Jako nejlepší příklad těchto zařízení jsou považovány tiskárny, servery a obecně zařízení, ke kterým se přistupuje ze sítě (9).

1.1.8 Bezpečnostní hrozby

Tato kapitola představuje základní bezpečnostní hrozby, které se v současnosti vyskytují. Dále také ukazuje, jak je nutné nastavit síť, aby byla schopna na ně správně reagovat nebo je včas odhalit, za účelem eliminace škod.

1.1.8.1 Útok Denial of Service

Denial of Service (zkráceně DoS) je útok, který je většinou využíván pouze jako nástroj k odvedení pozornosti od hlavní události, která probíhá v pozadí. Z toho incidentu útočník většinou nezíská žádné důležité informace ani kontrolu nad napadenou sítí. Jeho princip je jednoduchý. Počítač (nebo síť počítačů – DDOS) koordinovaně posílá obrovské množství požadavků na server napadnuté sítě. V případě, kdy je kapacita serveru dosažena nebo překročena, z pravidla zkolabuje a přestane odpovídat na další požadavky. Tento stav většinou vyústí v další útoky jiného typu využívající částečný nedostatek služeb. Pro lepší představu, vyřazením serveru mohla být oslabena bezpečnostní opatření a síť se stává zranitelnou. Dalším důsledkem bývá finanční poškození napadnuté společnosti díky nedostupnosti jejich služeb (10; 11).

Detekce a zastavení DoS a DDoS útoku je velmi obtížné, ale možné. Je nutné mít zavedené sledování sítě a analýzu přicházejících požadavků. V případě, kdy se začnou vyskytovat anomálie, je lepší reagovat, i když by se mohlo jednat o falešný poplach. Může se stát, že bude společnost mírně finančně poškozena kvůli výpadku svých služeb. Pokud je ovšem útoku zabráněno, znamená to pro ni, ve většině případů, vyhnutí se bezpečnostnímu incidentu, který by nejspíše následoval. Kdyby v opačném případě k incidentu došlo, může být finanční škoda astronomicky vysoká (11).

1.1.8.2 Spam

Spam je nejčastěji reklamní sdělení šířené pomocí komunikačních kanálů. Ve velké míře jsou to například e-maily, ale začínají se připojovat i zprávy na sociálních sítích. Většina zpráv šířených tímto způsobem je neškodná a není schopna síť ohrozit. Malé procento ovšem může být nositelem viru nebo malware, který je navržený na napadnutí počítače nebo celé sítě. V tomto případě už vzniká bezpečnostní incident (12).

Se spamem je spojený i pojem botnet. Jedná se o síť automatických nebo autonomních počítačů, které vědomě či nevědomě vykonávají určitou činnost. V tomto případě rozesílají spamy. Tyto sítě počítačů mohou být vytvořeny například po napadení počítačů malwarem, který se dokáže šířit právě v síti. Nežádoucím důsledkem botnetu je nedůvěryhodnost sítě pro ostatní entity nacházející se na internetu (12).

Detekce a zabránění spamu spočívá ve správném nastavení emailového serveru. Z toho důvodu je doporučováno pro firemní prostředí využívat vlastního emailového serveru a domény. Díky tomuto opatření je možné snížit nebo při správné implementaci úplně eliminovat výskyt incidentu. Dalším důležitým aspektem je školení zaměstnanců, což působí jako nejlepší prevence již zmíněného problému (12).

1.1.8.3 Slovníkové útoky

Slovníkové útoky spočívají v hrubém napadání systémů a pokusech o prolomení hesla. Jejich název je odvozen od způsobu, jakým útok probíhá. Jsou tu dvě možnosti. První možnost je zkoušení hesel podle databáze (slovníku), která je předem definovaná. Není to tak přesná metoda, jelikož se spoléhá na existenci hesla v databázi. Pokud je však databáze správně zvolena může být časově efektivnější. Druhá možnost spoléhá na hrubou metodu, kde je nadefinován nejmenší a největší počet znaků, které předpokládané heslo obsahuje. Poté se klient připojuje k systému a zkouší podle nastavených pravidel přihlašování pomocí hesel, která se mění podle nastavených pravidel. Metoda je velmi časově náročná, ale v případě správně nastavených pravidel velmi přesná (12).

Obrana a detekce podobných způsobů napadení sítě přichází již v případě prevence, kdy je heslo nastaveno podle doporučené složitosti. To znamená dostatečnou délku, obsah malých a velkých znaků, číslic a speciálních znaků. Při dodržení těchto pravidel se násobně zvyšuje počet permutací a díky tomu se snižuje pravděpodobnost prolomení hesel (12).

Velmi častou a vyžadovanou technikou je vícefázová autentifikace, jejíž výhodou je ideálně zapojit do procesu ověření více nezávislých zdrojů informací o uživateli. Typické způsoby implementace vícefázové implementace je odeslání SMS s ověřovacím kódem, nutnost připojení zabezpečeného USB klíče nebo ověření otisku prstu. Tyto doplňující informace je velmi složité odchytnout a slouží jako velmi účinný způsob zabezpečení (13).

Po určitém počtu neúspěšných přihlášení je další variantou časově odložit možnost dalšího přihlášení. Tímto se výrazně zpomalí postup útoku a zlepší zabezpečení sítě. Zároveň je tu možnost sledování logů zaznamenávající počty přihlášení do systému a započítávání neúspěšných pokusů (12).

1.2 Penetrační testování

Podstatou penetračního testování je napadnutí zabezpečené aplikace, systému nebo sítě. Na základě výsledků z těchto testů se vyhodnocuje úroveň zabezpečení. Metodika tohoto testování je založena na vyhledávání slabých míst a poté začíná snaha o využití těchto slabin k nabourání systému a pokus o získání co největšího oprávnění v rámci systému. Jako poslední krok v procesu zbývá interpretace bezpečnostních rizik a v závislosti na jejich vážnosti jsou rizika ohodnocena a reportována klientovi (14; 15).

1.2.1 Hledání slabých míst

Tato činnost je odvozena z anglického pojmu „vulnerability assessment“, tento pojem lze přeložit jako vyhodnocování zranitelností. Hledání slabých míst není stejný proces jako penetrační testování. Je to pouze dílčí činnost, která probíhá během celého testu. Tato činnost většinou s dnešními moderními nástroji po zadání potřebných údajů a správném nakonfigurování nástrojů probíhá automaticky (16).

Typické činnosti vykonávané těmito nástroji:

- procházení všech portů a služeb v celém rozsahu IP adres,
- zjišťování co největšího množství nastavení, zabezpečení, autentizace aplikací nebo služeb,
- zjišťování verzí, aktuálnosti a poslední bezpečnostní záplaty u operačních systému a aplikací,
- v případě pokročilejších nástrojů mohou probíhat i pokusy o napadnutí uživatelských účtů, pomocí hrubé metody prolomení hesel (hádání hesla a pokusy o přihlášení),
- po dokončení jejich úkolu poskytnou celkový report o stavu systému (16).

Výsledky testů jsou poté doplněny testující osobou o vyhodnocení jednotlivých hrozeb. Na základě tohoto hodnocení je rozhodnuto, které slabá místa mohou znamenat případný bezpečnostní incident. Při vyhodnocení je také nutné brát v potaz využití systému. Co je velkým rizikem pro zabezpečenou síť, může být pro síť menšího rozsahu zanedbatelné riziko. Nejčastější slabá místa v systému jsou většinou zapříčiněna přímo administrátorem. Jsou to neaktuální software a firmware, slabá hesla pro přístup do zařízení nebo špatně nakonfigurované porty na přepínačích (14).

1.2.2 Typy testů

Testy je možné dělit z různých hledisek. Nejčastěji používané rozdělení testů je na interní a externí (17).

- **Externí testy** jsou prováděny z volného internetu a v případě úspěšného napadení systému představují mnohem větší riziko než testy interní. Techniky těchto testů jsou založeny na znalostech chyb, které se vyskytují v různých typech a verzích technologií např. serverech, webových stránkách. Jelikož jsou tyto chyby již známé (databáze bezpečnostních slabin) je pro úspěšný útok dostačující znát programové nebo technologické vybavení napadnutého subjektu. Poté pouze mířit na již známou slabinu, která se v systému vyskytuje, a ještě na ni nebyla vydána bezpečnostní záplata. Jejich praktický význam je v podstatě útok hackera z internetu (17).
- **Interní testy** jsou prováděny z prostoru uvnitř sítě, napodobuje útočníka, kterému se podařilo získat fyzický přístup do serverovny nebo se jiným způsobem připojit do interní sítě (17).

1.2.2.1 Podle způsobu provedení

- **Automatizované testy** jsou prováděny nástroji, které jsou od základu navrhovány pro penetrační testování. Je to nejčastěji používaný systém testů, jelikož jsou časově a finančně nejvýhodnější. Jejich nevýhodou je menší přesnost závislá na komplexnosti nastavení jednotlivých testů a nemožnosti provádění testů s nutností uživatelského vstupu (16).
- **Manuální testy** jsou vykonávány osobně testerem. Jeho velkou výhodou je možnost nastavení testu na míru pro každou unikátní konfiguraci sítě. Největší nevýhodou je cena, která bývá vysoká kvůli velké časové náročnosti. Další nevýhodou je faktor člověka v procesu, celkový výsledek závisí na znalosti a zkušenosti testera (16).
- **Semi-automatizované testy** jsou kombinací výše zmíněného a z hlediska všech výhod i nevýhod nejlepší cestou pro spolehlivé a zároveň cenově výhodné testování. Díky těmto vlastnostem jsou také nejvíce využívané (16).

1.2.2.2 Podle úrovně znalostí o systému

- **Black-box test** testovaný systém je považován za neznámé prostředí. Útočník se snaží napadnout systém, o kterém má minimum informací. Nezná vnitřní uspořádání, použitá zařízení ani úrovně zabezpečení. Všechny informace, které pro tento test má jsou informace dostupné veřejně na internetu. Může jít o informace běžně dostupné např. DNS nebo informace, které jsou získané např. z nějakého bezpečnostního incidentu, typicky únik dat. Tato metoda je nejtěžší možnou a simuluje napadnutí systému hackerem z internetu (17).
- **White-box test** je v podstatě opakem Black-box testu. Testerovi jsou známé rozšířené znalosti o systému a na základě těchto znalostí se snaží určit, kde by se mohlo nacházet slabé místo. Tento postup je ze začátku testu čistě teoretický a po vytvoření několika hypotéz je přenesen do praxe. V průběhu testu mohou vyplynout další poznatky, na kterých je postaveno další testovaní. Výhodou tohoto způsobu je hlubší znalost systému a díky tomu komplexnější výsledky testování (17).
- **Grey-box test** kombinuje předchozí postupy. Testerovi jsou poskytnuty základní informace, které je schopen nashromáždit jako více zapojený uživatel nebo běžný zaměstnanec. Nadále se chová jako útočník a snaží se využít těchto znalostí tím nejlepším způsobem (17).

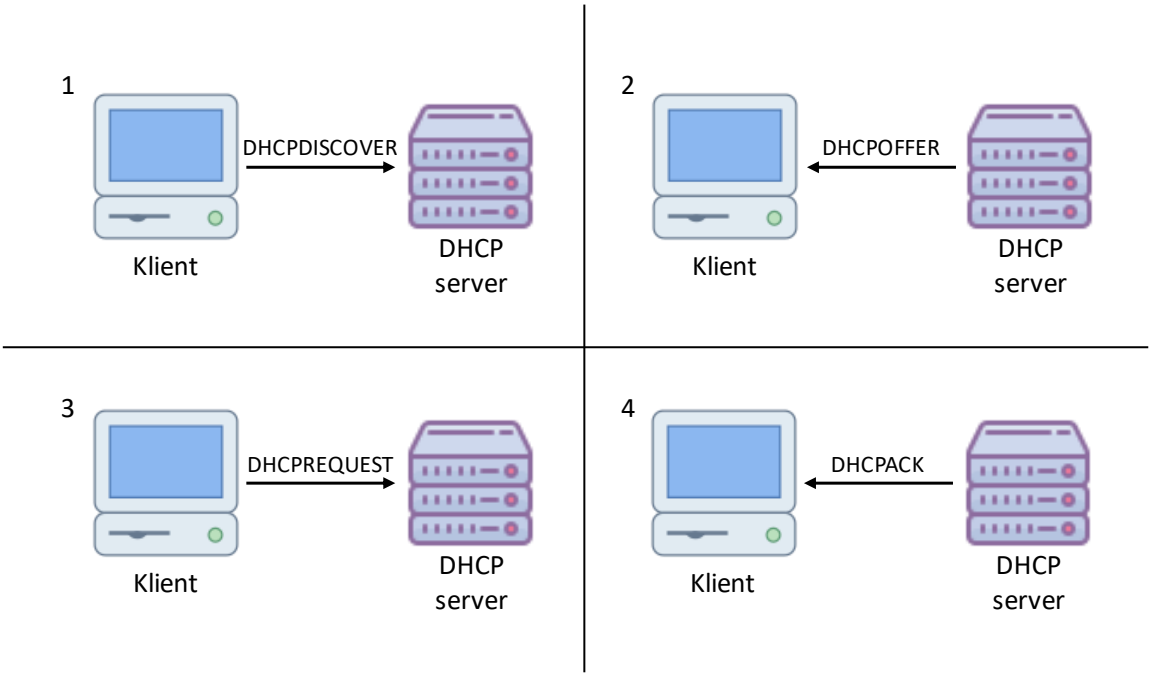
Každý z těchto testů je koncipován jiným způsobem a podává jiný výsledek. Pokaždé se jedná o úplně odlišný pohled, který simuluje jiný typ napadnutí sítě, z tohoto důvodu je doporučeno pro co největší komplexnost testu provádět všechny tři přístupy (17).

1.3 Principy vybraných síťových útoků

Tato kapitola rozebírá několik principů, které jsou využívány při napadání sítí. Jsou zde nastíněny principy, díky kterým jsou tyto techniky použitelné a pomáhají lépe pochopit techniky, které by mohly být využity v této diplomové práci později, konkrétně v analytické části.

1.3.1 DHCP spoofing

Dynamic host configuration protocol (zkráceně DHCP) je protokol, který umožňuje dynamické poskytování IP adres pro zařízení, která jsou nově připojená do sítě. Tím je provedena první a základní konfigurace zařízení, aby s ním bylo možné komunikovat. Proces je zahájen klientem, který do sítě vyšle broadcastový packet DHCPDISCOVER, který je vyslán na IP adresu 255.255.255.255. Tím je DHCP server vyzván, aby na požadavek reagoval a ten odpovídá packetem DHCPOFFER, kde poskytne klientovi potřebné informace zmiňované výše. V případě, kdy je v síti více DHCP serverů může klient dostat těchto odpovědí více. Pak reaguje vždy na první přijatou. Reakcí na packet DHCPOFFER je packet DHCPREQUEST, který potvrzuje DHCP serverů jeho výběr a ten následně reaguje zasláním posledního packetu DHCPACK, který klientovi potvrzuje jeho výběr a ukončuje celý proces konfigurace. Tento proces je graficky znázorněn na obrázku níže (18).



Obrázek 4: Diagram konfigurace IP za pomoci DHCP (19).

Tento princip zneužívá technika DHCP Spoofing, pomocí útoku Man in the middle (MiTM), a to tak, že útočník pošle falešný packet DHCPOFFER, který doručí dříve než správný DHCP server. V tomto packetu je místo IP adresy DHCP serveru adresa útočníka. Man in the middle se chová jako mezistanice na cestě od oběti k DHCP serveru.

Díky tomu je útočník schopen monitorovat všechnu komunikaci oběti směřující na výchozí bránu. Pro dosažení možnosti zachytávat i přijatou komunikaci je možné využívat techniky překladu adres NAT nebo současně s falešnou IP adresou podstrčit i falešnou adresu DNS serveru a tento odposlech provádět na něm (20).

Aby se tato technika podařila, jsou tu tři možnosti:

1. Snažit se odpovědět na DHCPDISCOVER packet dříve, než DHCP server a pokusit se, aby DHCPOFFER vypadalo jako legitimní odpověď, což je v případě, kdy zařízení v síti již někdy bylo připojeno, značně nespolehlivé,
2. Dále je možnost záměrně vyčerpat všechny IP adresy, které se nachází v rozsahu poskytovaném DHCP serverem, který díky tomu přestane následně další adresy přidělovat,
3. A poslední variantou se DHCP server úplně vyřadit. Nabízí se nám tu například DoS útok, kdy je server požadavky tak zahlcen, že může dojít dlouhé době odezvy na zasílané požadavky nebo dokonce k restartu (20).

1.3.1.1 Detekce útoku DHCP spoofing

Odhalení falešného DHCP serveru lze provézt několika způsoby:

První způsob detekce je mít v síti aktivní prvek, který bude „počítat“ množství odpovědí DHCPOFFER po odeslání jednoho dotazu DHCPDISCOVER. A to pouze v případě, kdy dochází ke konfiguraci nového zařízení. Pokud je po odeslání obdrženo více než jedna odpověď, je jasné, že se v síti nachází více než jeden DHCP server (20).

Druhý způsobem je aktivní generování paketů DHCPDISCOVER (v pravidelných intervalech) a kontrolování odpovědí DHCPOFFER. Tohle ověření provádí přímo DHCP server. Tento postup však není moc dobré řešení, a to hned z několika důvodu. Zbytečně si zatěžujeme síť a DHCP server, a navíc je lehko detekovatelný případným útočníkem (21).

1.3.1.2 Obrana proti útoku DHCP spoofing

Nejjednodušší obranou proti tomuto útoku je nepoužívat DHCP server (tedy nastavit IP adresy staticky), ale ve firemním prostředí není tato varianta vždy možná, jelikož se na pracovištích střídá velké množství zařízení (21).

Je zde možnost sofistikovanější obrany, která však vyžaduje investici do specializovaného hardware nebo v případě Cisco přepínačů vyšší řady jejich zařízení, které tuto funkcionalitu nativně podporují. Jde o využívání funkce DHCP snooping, která aktivně monitoruje celý proces DHCP a pokud zachytí jakoukoli podezřelou odpověď, tak ji zastaví. Jsou zde i jiné varianty, ale většinou fungují na stejných principech akorát jsou prodávané pod jinou značkou (20).

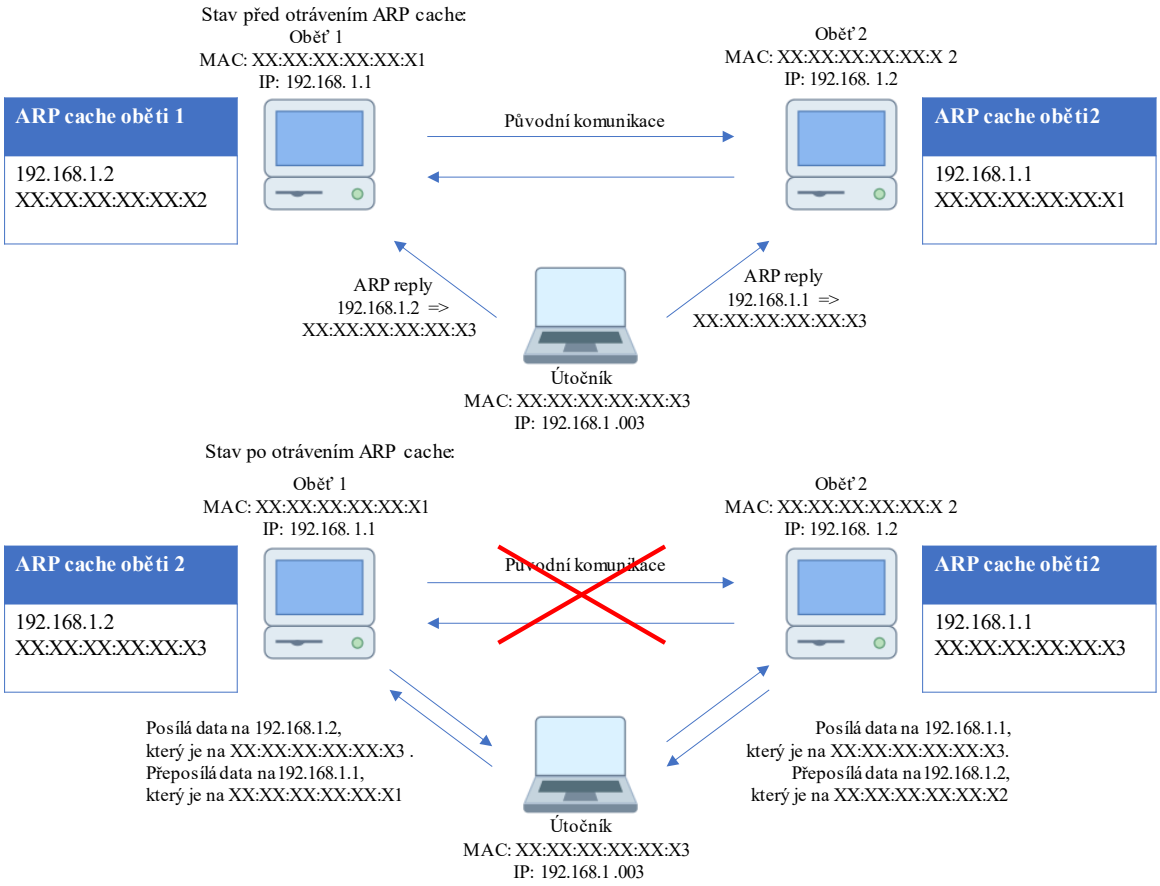
1.3.2 ARP Spoofing

Address Resolution Protocol (ARP) je protokol zajišťující spojení mezi linkovou a síťovou vrstvou v modelu TCP/IP. Funkcí tohoto protokolu je překlad lokálních IP adres na MAC adresy síťových uzlů. V případě, kdy chce jakékoli zařízení v lokální síti komunikovat s nějakým jiným ve stejné síti je nutné, aby si nejdříve získalo MAC adresu cílového zařízení. Proces začíná vysláním packetu ARP request neboli žádost o MAC adresu, která přísluší k určité IP adrese. Příjemcem tohoto packetu jsou všechna zařízení v rámci lokální sítě. Zařízení, kterému náleží IP adresa z tohoto dotazu poté odpoví dotazovateli unicastovou zprávou ARP reply, která obsahuje MAC adresu cílového zařízení. Tato vazba mezi IP a MAC adresou je uchováno do ARP cache z důvodu minimalizování nutnosti odesílat další ARP requesty (22).

Princip útoku ARP spoofing nebo též ARP cache poisoning využívá faktu, že IP adresa, která je uvedena v hlavičce packetu nemusí odpovídat skutečné adrese zdrojového zařízení. Další skutečností, je že ARP protokol je bezstavový, to znamená, že lze zaslat odpověď bez toho, aby o ni bylo zažádáno. Díky tomuto faktu je možné, aby se útočník postavil mezi příjemce a odesílatele dat. Útočník odešle příjemci i odesílateli falešný ARP reply, ve kterém je místo záznamů příjemce a odesílatele záznam útočníka. Tento záznam je zapsán do ARP cache a nadále bude probíhat vzájemná komunikace prostřednictvím útočníka a tímto způsobem je útočník schopen zachytávat vzájemnou komunikaci. Útočník už si musí jenom nadále zajistit, aby záznam z ARP cache nebyl vymazán,

jelikož tyto záznamy mají svoji dobu expirace. Tohle se zajistí pravidelným odesíláním ARP reply na obě oběti (23).

Na obrázku pět je princip útoku zobrazen graficky pro lepší pochopení. V první polovině je zobrazeno, jakým způsobem se útočník infiltruje do komunikace obětí. V druhé polovině je zobrazeno již hotové nabourání komunikace při úspěšném útoku.



Obrázek 5: Princip útoku ARP Spoofing (17).

1.3.2.1 Detekce útoku ARP spoofing

Detekce útoku ARP spoofing je možné provádět na straně přepínače nebo na straně uživatele. V případě, kdy je potřebné aktivně detekovat útoky na straně přepínače, tak budeme většinou potřebovat spravovatelný přepínač, který tuto funkcionalitu nabízí. Jinak tuto funkci nabízí i většina dostupných a využívaných firewallů. Samotná detekce probíhá jednoduše, a to srovnáním ARP tabulky s reálným stavem, který je aktuálně v sítí.

Druhá možnost je hlídat packety ARP reply. Pokud se v sítí objeví packet ARP reply bez toho, aniž by byl odeslán packet ARP request je jasné, že se v síti nachází útočník snažící se o její napadnutí.

Pro uživatelskou detekci existuje několik programů např. Wireshark, tshark, XARP a další, které obdobným způsobem jako přepínač analyzují síť a její provoz. Na základě těchto pozorování vyhodnocují stav a případně upozorní na útok. Tato náhrada je sice použitelnou alternativou, ale není to dokonalé řešení. Detekce je pomalejší a méně spolehlivá, také vyžaduje, aby měl přepínač přístup do všech virtuálních sítí na lokální síti, a to není z hlediska další bezpečnosti vhodné (22).

1.3.3 MAC flooding

Síťový útok MAC flooding využívá zranitelnosti ve fungování přepínačů. Přepínač přeposílá rámce v sítí vždy přímo na konkrétního příjemce podle MAC adresy, které je rámec adresován. Tohle směrování je udržováno tzv. CAM tabulce, která obsahuje propojení MAC adresy s cílovým rámcem. Pokud je tento záznam v tabulce nalezen je zaslán rámec na konkrétní port. Pokud to tak není je rámec odeslán na všechny dostupné porty kromě toho odkud přišel. Na tomto principu je postaven útok (23).

Záznamy do CAM tabulky jsou postupně přidávány v průběhu reálného provozu sítě. V případě, kdy je přijat rámec z portu, který nemá v tabulce žádný záznam, je tento port do tabulky přidán. Nadále je tento princip používán z důvodu zvýšení rychlosti a snížení vytížení sítě. Tento záznam má určitou dobu expirace a musí být poté obnoven. Pokud záznam není obnoven, dochází k jeho smazání, aby se v tabulce udělal prostor pro další záznamy, jelikož má tabulka omezenou kapacitu je to nutnou podmínkou. A právě tohoto faktu se využívá při útoku. Útočník se přihlásí do sítě a začne rozesílat náhodné rámce z náhodně vygenerovaných MAC adres. Přepínač začne reagovat tak jak by měl a začne zaplňovat CAM tabulku novými záznamy. Až dojde k úplnému naplnění tabulky, přepínač do ní přestane zapisovat další data a přestane ji používat. Přepne se do fail open režimu, jehož funkce umožňuje další fungování sítě za cenu toho, že směrovač přestane směrovat a začne se chovat jako obyčejný rozbočovač. Pro běžná zařízení to znamená pouze mírné zpomalení odezvy, ale pro útočníka, který má síťové rozhraní nastavené do režimu, kdy přijímá všechny rámce, to znamená úspěšné napadení sítě. Útočník má díky tomu možnost začít odposlouchávat komunikaci v rámci sítě, a to jak příchozí, tak

odchozí. Tento stav však není dlouhodobě udržitelný, pokud útočník přestane přepínač zahlcovat novými požadavky s novými MAC adresami, tabulka se sama uvolní a přepínač se vrátí do původního stavu (23).

1.3.3.1 Obrana a detekce útoku MAC flooding

Obrana proti tomuto útoku je jednoduchá a velmi účinná. Je pro ni využíváno mechanismu port security, kdy je dán maximální počet MAC adres připadající na jednotlivý port. Po dosažení tohoto limitu, již nejsou do tabulky přidávány další záznamy pro tento port a není možné, aby došlo k jejím přeplnění (23).

Detekce tohoto útoku je poměrně složitý proces. Nejjednodušší metodou pro detekci je zjištění celkového počtu zaslaných rámců za určitou dobu a počet unikátních MAC adres, ze kterých přišli. Pokud je tento počet porovnatelný, tak se pravděpodobně nejedná o běžný síťový provoz, ale o útok (23).

2 Analýza současného stavu

V této části se práce věnuje analýze a měření současného stavu technologie a vybavení klienta. Dále je tu představeno testovací centrum, na kterém probíhá celé testování a prostředky, které jsou pro tohle testování vynaloženy. Dále jsou zde rozpracovány tři hypotézy a metodiky, pomocí kterých se bude řídit reálné testování. Tyto hypotézy a metodiky byly formovány s přibývajícími znalostmi ohledně toho klientského řešení.

2.1 Testovací prostředí

Pro lepší pochopení je potřeba si představit zařízení a technologie, které byly využity pro testování a kopírují vybavení běžného kancelářského centra této firmy. Jediným rozdílem je nezařazení do sítě zařízení, která nejsou pro tohle testování nutná: např. Wi-Fi přístupový bod, Callstream server, kamery. Pro tohle centrum byly vytvořeni i noví virtuální klienti, z důvodu citlivosti testů, které mohou teoreticky ohrozit integritu datové bezpečnosti klientů reálných. Vše v rámci tohoto testovacího prostředí je uzpůsobeno tak, aby neohrozilo síťovou a informační bezpečnost, ale zároveň co nejpřesněji kopírovalo reálné síťové prostředí. Tohle testovací centrum se nachází v brněnském logistickém centru společnosti Dworkin spol. s r.o. Od této společnosti jsou využívány i další zdroje. Tyto zdroje jsou v oblasti fyzického hardware, znalostí a času věnovaného jejich dalšími zaměstnanci pro měření a případnou výpomoc s touto diplomovou prací.

2.2 Základní informace o společnosti Dworkin spol. s r.o.

Společnost Dworkin, spol. s r.o. podniká v odvětví informačních technologií. Jejím sloganem je „ IT is all about people“ v překladu „IT je o lidech“. Společnost vyrostla do korporace, avšak se snaží být v co nejvíce možném měřítku jako rodinná. Klade důraz na to, že obor informačních technologií není jen o zařízeních, programování a zapojování kabelů, ale že je hlavně o lidech a správnému jednání s nimi. Důležité je umět pomoci lidem s jejich IT problémem.

Společnost se může pyšnit dlouhou historií působnosti na trhu. Založena byla 21. listopadu 1995 v Praze. Může se tedy pyšnit více jak 25 lety zkušeností. V současné době zažívá velký rozmach a růst, svoje služby nabízí ve více jak sedmdesáti zemích celého světa. Navíc je schopna poskytovat podporu díky velkému počtu zaměstnaných techniků. V současné

chvíli přímo zaměstnává přes 150 techniků a administrativních pracovníků po celém světě. Dále je tu dalších až 30 kontraktorů v zemích, které mají menší hustotu klientů a menší odbyt pro poskytované služby, a navíc jsou to země, které nemají pokročilé firemní zázemí. Tito kontraktoři jsou zastoupení jako jedinci a v některých zemích jako např. Turecko, Izrael nebo Skotsko dokonce celé společnosti (24).

V posledních letech společnost začala posilovat svoje postavení v oblasti logistiky a byla založena tři nová logistická centra. Jedno, které již v Brně bylo, se přesunulo do větších a modernějších prostorů a byla vytvořena dvě další – jedno ve Velké Británii pro poskytování služeb pro Anglii, Skotsko, Wales a Severní Irsko. A druhé v Nizozemsku s plánem na pokrytí zemí Beneluxu a části západní Evropy. Tohle poslední logistické centrum je v současné době ve fázi výstavby. Jeho úplné uvedení do provozu se očekává v srpnu 2021.

Obrázek 6: Logistické centrum Dworkin Brno

Velkou předností této firmy je možnost přizpůsobení dodávky technologie podle požadavku zákazníka. Tento proces je interně nazvaný prestaging a spočívá v přípravě zařízení pro instalaci u zákazníka bez dalšího nutného nastavení, takzvané plug & play. Takto připravované zařízení jsou přepínače, servery nebo v některých příkladech i celé rozvaděče.

Název: Dworkin spol. s r.o.

Sídlo: Rohanské nábřeží 657/7, Karlín, 186 00 Praha

Datum založení: 21. listopad 1995

Právní forma: společnost s ručením omezeným,3

Statutární orgán: Ing. Martin Křivý

Základní kapitál: 100 000,- Kč

Obrázek 7: Logo společnosti Dworkin spol. s r.o. (24).

2.2.1 Testovací hardware

Pro úspěšné provozování technologie ANC, jejíž úplná funkčnost je nutným předpokladem, pro schopnost začít s testy vytvořených hypotéz, je zapotřebí infrastruktura postavená z následujícího hardwaru: firewall Clavister E80 a přepínač Cisco Catalyst 2960X-24TS-L pro hypotézy číslo dvě a tři. Pro hypotézu jedna bude nasazen zastaralý hardware se zastaralým firmware a bude se jednat o Clavister SG60 a Cisco Catalyst 3560X-24T-S.

Obrázek 8: Clavister E80 – firewall.

Obrázek 9: Cisco Catalyst 2960X-24TS-L – přepínač.

Obrázek 10: Clavister SG60 – firewall.

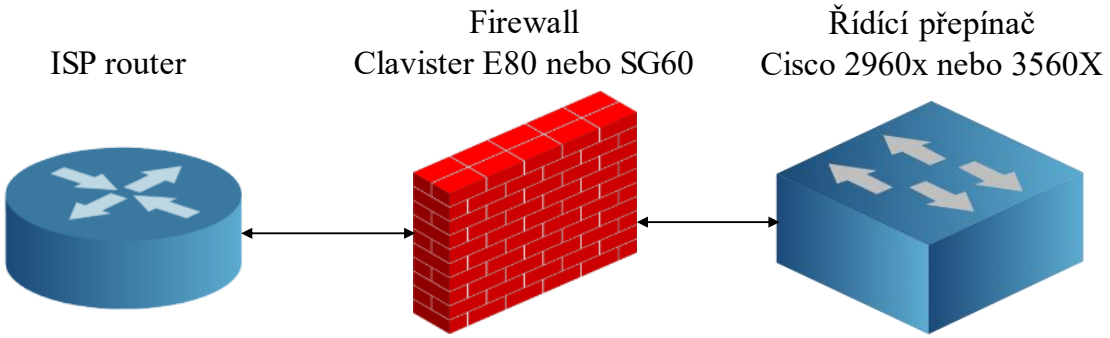
Obrázek 11: Cisco Catalyst 3560X-24T-S – přepínač.

Pro samotné testování a vyhodnocování budou využity tři počítače. Dva stolní, které budou každý registrovaný do virtuální sítě jiného klienta. Na těchto počítačích bude předvedena funkčnost technologie pro logické rozdělení sítě na několik virtuálních podsítí. Třetí počítač, což bude notebook vybavený USB-C rozhraním a pro připojení do počítačové sítě bude využívat adaptér i-tec (USB-C na Ethernet), který umožňuje jednoduše měnit MAC adresu přímo v prostředí Windows. Tím je možné dosáhnout možnosti, kdy jeden notebook ze strany sítě bude působit jako dvě odlišné zařízení.

Obrázek 12: USB-C Gigabit Ethernet Adapter.

2.2.2 Topologie testovacího centra

Topologie testovacího centra je velmi jednoduchá. Obsahuje pouze nutné množství hardwaru potřeného k úspěšnému testu technologie ANC. Do topologie je zahrnutý i ISP směrovač, který ovšem není fyzicky ani vzdáleně přístupný, jelikož je ve správě poskytovatele internetu, a navíc je umístěn ve vedlejší budově. Na obrázku 12 je zobrazena topologie pro všechny případy testování, obě verze zařízení podporované i nepodporované.



Obrázek 13: Topologie testovacího centra.

2.3 Analýza informačního systému

Tato část práce se zabývá analýzou zabezpečení a uživatelské přívětivosti celého systému, který zapisuje, spravuje a zabezpečuje celkovou správu databáze MAC adres a VLAN zařízení. Pro vypracování analýzy bylo využito nástroje Zefis, pomocí kterého byla vyhodnocena efektivita a bezpečnost celého systému a základních ukazatelů společnosti.

Během této analýzy byly objeveny menší nedostatky, které jsou způsobeny horší uživatelskou přívětivostí a některými dalšími problémy ohledně zabezpečení. Úkolem této analýzy nebylo hodnotit systém přiřazování MAC adres a hodnotí pouze doprovodný systém, který se stará o udržování databáze a přístup do něj.

V kapitolách níže, které se věnují určité části systému a hodnotí její bezpečnost nebo efektivitu užití, jsou rozebrány jednotlivé nedostatky, je zde zhodnoceno a vysvětleno, z jakého důvodu nastala tato neshoda a jak je vnímána z hlediska bezpečnosti ANC. Navíc hodnotí i technologie, které jsou na tuto technologii navázané.

2.3.1 Výsledky analýzy společnosti

V této části analýzy byla obecně zkoumána společnost z pohledu bezpečnosti. Tato analýza se zabývá pouze základními informace a popisuje všeobecné a nejcitlivější aspekty bezpečnosti v rámci společnosti.

Tabulka 1: Výsledky společnosti.

Významnost	Neshoda
N16 – Vysoká	Chybí strategie bezpečnosti
N20 – Vysoká	Bezpečnostní hrozba virového útoku
N10 – Střední	Zastaralé technické vybavení

2.3.1.1 Rozbor neshod analýzy společnosti

- **N16 | Chybí strategie bezpečnosti** – tento problém se nevztahuje přímo na systém, ale na celkovou strategii pro zajištění a dodržování bezpečnosti. V rámci strategie by měla být zpracována pravidla pro zaměstnance a také směrnice pro vnitropodnikovou bezpečnost.
- **N20 | Bezpečnostní hrozba virového útoku** – jelikož jeden z výstupů analýzy bylo, že společnost nevyužívá celopodnikovou implementaci bezpečnostního antivirového programu a spoléhá na znalosti svých zaměstnanců, je nutností takové řešení co nejrychleji implementovat. A to z důvodu dalších funkcí, které takové řešení nabízí. Jako např. pokročilý firewall, ochrana proti napadnutí škodlivým flash diskem a možnost kontroly všech souborů z emailů a podobných způsobů komunikace.
- **N10 | Zastaralé technické vybavení** – v případě některých center se stává, že je vybavení recepce zastaralé, a to jak hardwarově, tak softwarově. Z hlediska software to znamená využívání operačního systému Windows 7 na přístrojích, které již Windows 10 nepodporují, ze strany hardwarové se jedná o zastaralé přepínače nebo obecně síťový hardware centra. Doporučení je zaměřit se v první fázi na co největší potlačení počítačů s nepodporovaným operačním systémem a poté vyřešit i ostatní problémy.

2.3.2 Výsledky analýzy systému

Tato část zkoumá samotný systém interakci s ním, a to včetně hardwaru, který je pro interakci se systémem určen. Navíc hodnotí design, výstupy ze systému a jejich vypovídající hodnotu pro klienty a zaměstnance.

Tabulka 2: Výsledky systému.

Významnost	Neshoda
N8 – Vysoká	Nízká kvalifikace pracovníků při práci s počítači
N45 – Nízká	Nevhodný design systému pro zákazníky

2.3.2.1 Rozbor neshod analýzy systému

- **N8 | Nízká kvalifikace pracovníků při práci s počítači** – jeden z problémů, který byl objeven v průběhu analýzy byla nízká kvalifikace zaměstnanců při práci s počítačem. Důvodem, proč je tato neshoda na vysoké úrovni neznalosti, je případný bezpečnostní problém, který může nastat neodborným zásahem do systému nebo sítě. Navíc pokud se jedná o přístup ke klientům, je velmi neprofesionální mít nevyškolené zaměstnance.
- **N45 | Nevhodný design systému pro zákazník** – pro tento případ se nejedná přímo o nevhodný design, ale spíše o design systému. V některých částech klientského portálu systému se objevuje nekonzistentní vzhled, který může vést ke zmatení uživatelů a snížení efektivnosti jejich práce.

2.3.3 Výsledky analýzy procesu

V této části je hodnocen proces vytvoření nové virtuální sítě pro užití klientem. Vyhodnocení je zpracováno v návaznosti na systém a zpětnou vazbu klientů.

Tabulka 3: Výsledky procesu.

Významnost	Neshoda
N66 – Střední	Chybí průzkumy spokojenosti zákazníků
N65 – Nízká	Není známo, jak jsou příjemci spokojeni s výstupy procesu

2.3.3.1 Rozbor neshod analýzy procesu

- **N66 | Chybí průzkumy spokojenosti zákazníků** – jelikož není zaveden způsob zpětné vazby pro informační systém od zákazníků, není v současné době možné reagovat na jejich potřeby a podněty. Do budoucnosti by bylo vhodné podobné nástroje implementovat a brát ohled na tyto ohlasy při implementaci nových aktualizací a funkcí.

- **N65 | Není známo, jak jsou příjemci spokojeni s výstupy procesu** – tento problém přímo navazuje na předchozí neshodu. V případě zavedení zpětné vazby pro klienty by měla být zavedena i pro interní zaměstnance pro ještě lepší rozsah informací, které se ze systému dají vytěžit pro co nejlepší porozumění problémům vyskytujících se v něm vyskytují.

2.3.4 Výsledky analýzy auditu užití

Tato část shrnuje celkovou efektivitu a bezpečnost systémů a dívá se na problematiku z širšího, obecnějšího pohledu.

Tabulka 4: Výsledky auditu užití.

Významnost	Neshoda
N59 – Střední	Pracovníkům chybí některá data nebo funkce
N85 – Střední	Bezpečnostní hrozba z přístupu na internet
N86 – Střední	Riziko zneužití dat, virového útoku
N83 – Nízká	Vyšší náklady na tisk

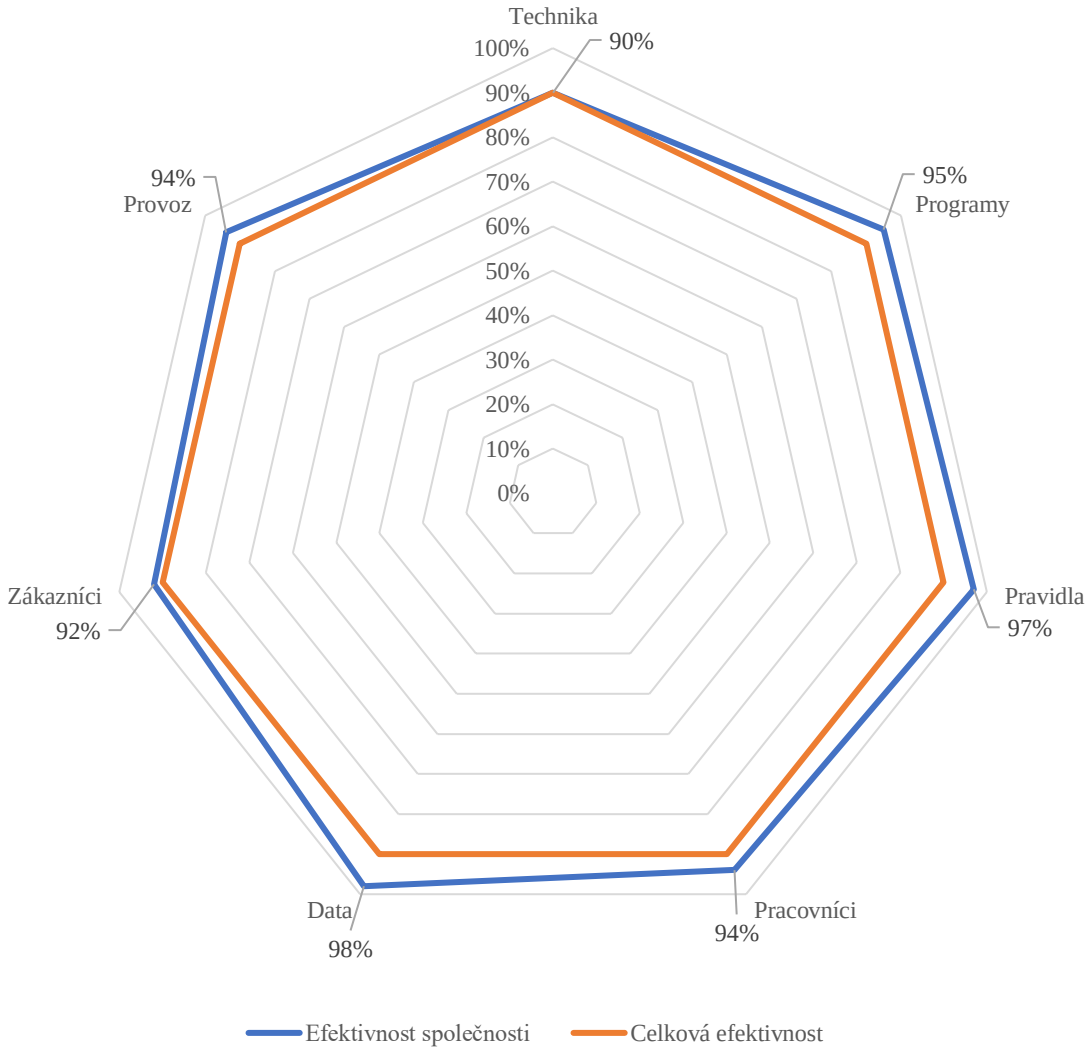
2.3.4.1 Rozbor neshod analýzy auditu užití

- **N59 | Pracovníkům chybí některá data nebo funkce** – tohle je problém navazující na předchozí kapitolu. Pokud zaměstnancům chybí nějaké nástroje nebo data je nutné, aby o tom věděl management systému a problém napravil. Nejlepší způsob, jak tohoto dosáhnout je opět pomocí zavedení zpětné vazby.
- **N85 | Bezpečnostní hrozba z přístupu na internet** – ano, přístup k internetu teoreticky představuje hrozbu, ale jelikož je to základní a nutný nástroj pro provádění přidělené práce není možné tento přístup zakázat.
- **N86 | Riziko zneužití dat, virového útoku** – tato neshoda je už také řešena výše, pro vyřešení problému je doporučeno aplikovat antivirový program pro všechny zaměstnance firmy. A zdůraznit potřebu obezřetnosti ohledně bezpečnosti při školení.
- **N83 | Vyšší náklady na tisk** – s touto neshodou se bude muset společnost smířit, jelikož je nutné, aby se v okolí recepce někdo ze zaměstnanců vždy vyskytoval nebo

byl alespoň v dosahu. V případě, kdy se na centru nachází sdílená tiskárna na jiném patře je nutné, aby byla tiskárna i přímo na recepci.

2.3.5 Efektivnost užití doprovodného systému pro ANC

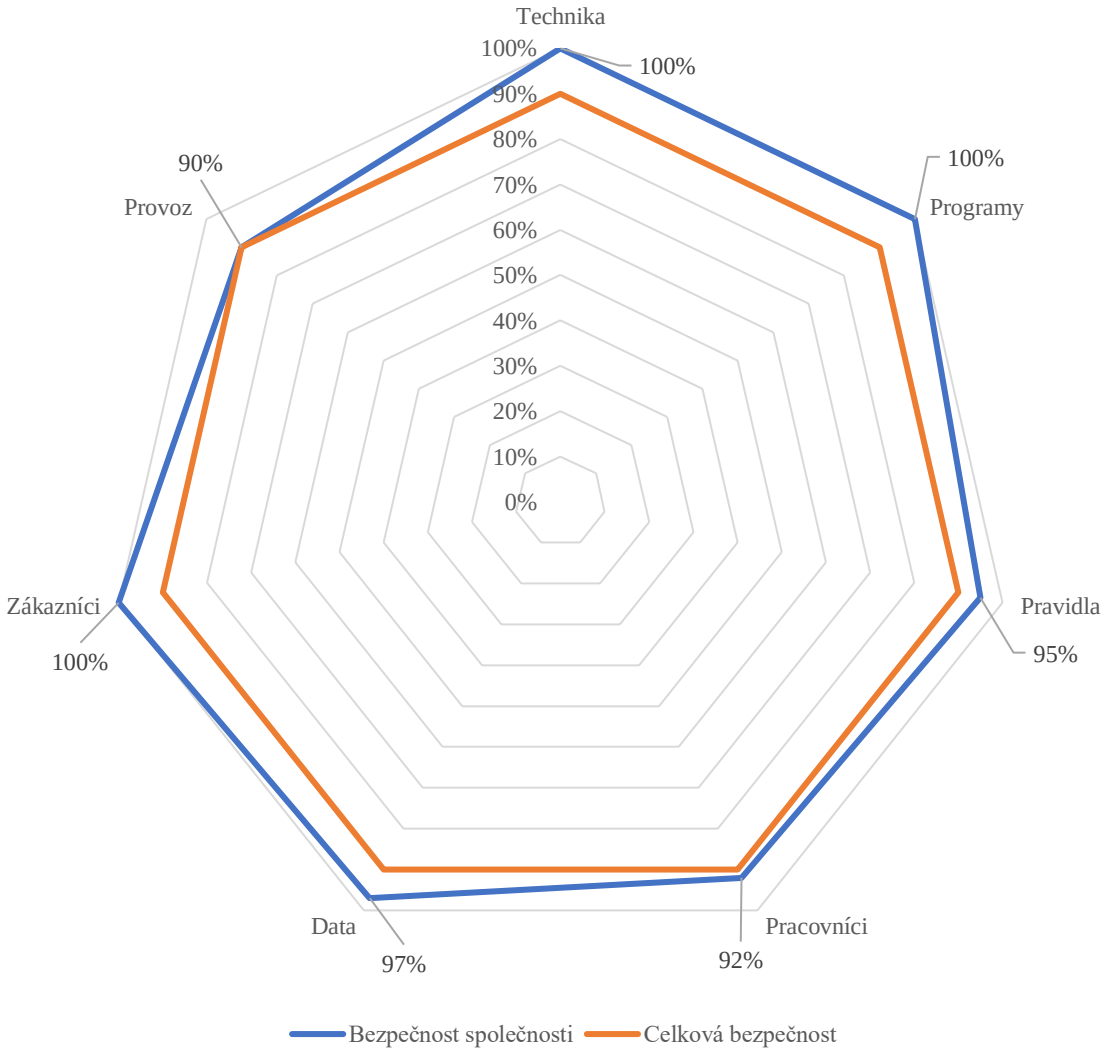
Z grafu 1 je vidět, že jelikož je oranžová linka, která ilustruje celkovou efektivnost celého systému, na 90 %, lze považovat celkovou efektivitu za velmi dobrou. Oblast, která podle analýzy omezuje efektivnost celého systému, je technika. To sice hned neznamená problém, ale je zde prostor pro zlepšení. Hlavním nedostatkem techniky je považováno její neúplné zabezpečení či v některých případech zastaralost.



Graf 1: Efektivnost užití doprovodného systému ANC.

2.3.6 Bezpečnost užití doprovodného systému ANC

Jak je vidět na grafu 2 z hlediska zabezpečení doprovodného systému pro ANC, nejnižší hodnota se zastavila také na 90%. To je velmi dobrý výsledek. Jak je vidět na obrázku, dílčí výsledky jsou v průměru dokonce lepší než v případě efektivity systému. Zákazníci, technika a programy jsou dokonce na 100 procentech, což neznamená, že není nutné dělat změny, ale znamená to, že v tento moment je vše v pořádku. Je zapotřebí vše monitorovat a vylepšovat všechny systémy současně z důvodu, že celková bezpečnost vždy záleží na nejslabším článku.



Graf 2: Bezpečnost užití doprovodného systému ANC.

2.3.7 Celkové zhodnocení analýzy informačního systému

Na základě analýzy informačního systému bylo vyhodnoceno, že systém pracuje s celkovou efektivitou 90% a na stejné úrovni je i jeho zabezpečení, což je velmi dobrý

výsledek. Menší nedostatky byly objeveny v oblasti efektivity, kde se jedná především o drobné designové nesrovnalosti v systému a neexistující zpětnou vazbu o fungování ze strany klientů a zaměstnanců.

Z hlediska zabezpečení se tu vyskytuje problém s nevyužíváním žádného antivirového klienta, který by zabezpečil jednotlivé pracovní stanice zaměstnanců. Dále se tu vyskytuje problém, který se týká zastaralého hardware, jak ve vybavení zaměstnanců, tak v síťové infrastruktuře.

2.4 Způsob přiřazování VLAN pomocí ANC

ANC je technologie využívající dynamického způsobu přiřazování VLAN na základě MAC adresy aktuálně připojeného zařízení. Způsob, jakým jsou tyto VLANy distribuovány je založen na databázi běžící v prostředí Microsoft Azure. V ní se uchovávají MAC adresy všech zařízení, která jsou přiřazena ke klientovi. Pro zaznamenávání a udržování jednotlivých klientů je zavedeno „Titan ID“, což je unikátní číselné ID pro každého klienta. Za pomoci tohoto ID se udržují v informačním systému všechny informace o každém klientovi, včetně účetnictví, smluv a MAC adres zařízení. Díky tomuto propojení mezi ID a MAC adresou zařízení se v případě, kdy má klient aktivovanou službu vlastní virtuální sítě, je mu tato virtuální síť po připojení do sítě přidělena a port na přepínači je automaticky nastaven na konfiguraci, která je pro něj v databázi uložena. Tato konfigurace zůstává aktivní, dokud je zařízení k portu připojeno. Po jeho odpojení se nastavení změní zpět na výchozí VLANu 980 (open port), která je určena pro zařízení pouze s přístupem k internetu bez možnosti vlastní virtuální sítě. Dále je tu poslední varianta a ta nastává, pokud je do sítě zapojeno zařízení, které není přiřazeno k žádnému klientovi a v databázi o něm nejsou žádné záznamy. V takovém případě je mu přiřazena VLANa 798, která omezuje komunikaci připojeného zařízení pouze na určité UDP porty a zakazuje tradiční přístup do internetu (25).

2.5 Analýza síťového prostředí

V případě, kdy bude potřeba zapojit další nástroje pro zabezpečení sítě je nutné, aby bylo známé reálné prostředí sítě a klientská zařízení, která ji využívají. Ve výsledku se může jednat o síť homogenní nebo heterogenní (26).

- **Homogenní síť** se vyznačuje využíváním jednotného operačního systému u koncových zařízeních, jednotným protokolem pro komunikaci mezi nimi a jednotným prostředím,

ve kterém komunikace probíhá. Taková síť je jednoduchá pro údržbu jak koncových uzlů, tak sítě. Navíc je jednodušší implementovat nové technologie a udržovat systém zabezpečený díky aplikování bezpečnostních záplat (26).

- **Heterogenní síť** se vyznačuje přesným opakem než homogenní síť. Koncová zařízení nejsou stejná a obsahují různé operační systémy v různých verzích. Tyto systému mohou být: Windows (10, 8, Vista atd.), Android (11, 10, 9 atd.), Linux (Ubuntu, Debian, Kubuntu), MacOS (11.0, 10.15, 10.14 atd.), iOS (14, 13, 12 atd.) apod. Navíc je síť provozována ve více prostředích Wi-Fi, kabelové připojení, což díky rozdílným vlastnostem těchto prostředí zvyšuje složitost sítě, její odezvu a v případě bezdrátového připojení i její spolehlivost (26).

2.5.1 Reálné síťové prostředí na centrech

Jelikož centra pro co největší pohodlí klientů kombinují kabelové a bezdrátové připojení pro zařízení je to již první předpoklad, proč lze síť považovat za heterogenní. Navíc, jde o služby poskytované pro mnoho klientů s různými potřebami a různými zařízeními, tím se síť ještě více diverzifikuje. To, co dělá síť velmi heterogenní je další dělení fyzické sítě na virtuální sítě pro jednotlivé klienty. Výsledkem je síť, pro kterou se těžko navrhuje jednotné řešení díky míře její heterogenity.

2.6 Přidělení zařízení k virtuálním klientům

Reálně bude testovaní probíhat na třech zařízeních, která jsou zaregistrována pod dva virtuální klienty. Virtuální klient 1 a Virtuální klient 2, nadále je pod Virtuálního klienta 1 přiřazena VLANa 500 a pod Virtuálního klienta 2 VLANa 600. Nadále je pod každou VLANu zaregistrovány pro VC1 jedno zařízení a pod VC2 tři zařízení. Pro lepší pochopení je toto rozřazení znázorněno v tabulce 5.

Tabulka 5: Přiřazení zařízení ke klientům.

Virtuální klient 1 (ID 11396705)	Virtuální klient 2 (ID 11396706)
PC1 VLAN 500 – MAC 00-E0-4C-68-1F-90	PC1 VLAN 600 – MAC 00-E0-4C-68-1F-91
PC2 – MAC 10-62-E5-17-09-5E	–
PC3 – MAC 34-99-71-D4-C8-34	–

Zařízení vypsaná v tabulce 5 jsou přiřazena jak ke klientovi, tak k určité VLANě. V ideálním případě při zapojení zařízení do sítě dojde k načtení správné VLANy z databáze a přiřazení k zařízení na přepínači. Výjimkou je zařízení PC1, které je přiřazeno k oběma klientům, ale pokaždé s jinou MAC adresou. Jedná se jedno fyzické zařízení v obou případech akorát jediným parametrem (MAC adresa), která se mění. Díky tomuto parametru vystupuje pro síťové prostředí jako dvě odlišná zařízení. Z toho důvodu může být zaregistrováno pod různými klienty. Zároveň bude toto zařízení figurovat jako útočník v celém procesu testování jednotlivých hypotéz.

Zařízení PC1 a PC2 jsou zaregistrována jako běžné klientské počítače. PC1 bude vystupovat jako klientské zařízení, které se pokouší narušit síť a bude vystupovat jako útočník. PC2 je tu bráno jako běžné zařízení, na které se zaměřuje útočník a vystupuje tu jako oběť. A zařízení PC3 bude do sítě přidáno jako monitorovací zařízení, které bude pasivně skenovat síť a zaznamenávat výsledky testů pro pozdější podrobnější analýzu.

2.7 Metoda zjišťování konfigurací portu z přepínače

Tato kapitola se pokouší přiblížit způsobu, jakým je získávána konfigurace z jednotlivých portů na přepínači. Pro tuto činnost je využíván další na testech nezávislý počítač, který je připojený pomocí konzolového portu k přepínači a s využitím programu Putty a příkazové řádky si nechává vypisovat jednotlivé konfigurace.

Na obrázku 14 je zobrazeno, jak takový příkaz vypadá, a jakým způsobem přepínač vypisuje požadovanou informaci. Pro lepší pochopení obrázku je třeba znát logiku pojmenování přepínačů v této společnosti. Na prvním řádku je vypsaný příkaz, kterým se žádá o vybranou informaci. V tomto textovém řetězci jsou dvě informace. Informace před znakem „#“ je jméno přepínače, o který se jedná a za ním o příkaz. Zbytek textu, už pouze vypisuje konfiguraci portu, ve které je zahrnuta VLANa, MAC adresa a číslo postu. Jestli je jedná o dynamický, či statický typ portu není pro tuto analýzu důležité.

```
SW00-15-01-2960.5693# show mac address-table int g1/0/13
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    2cea.7f78.f095    STATIC      Gi1/0/13
Total Mac Addresses for this criterion: 1
```

Obrázek 14: Vypsaná konfigurace portu 13.

2.8 Nástroje využívané pro testování hypotéz

Následující nástroje jsou využívány pro analýzu a vyhodnocování nalezených dat. Všechny tyto nástroje jsou volně dostupné a volně šiřitelné bez nutnosti pořizovat licence. Jedinou podmínkou pro užití těchto nástrojů je jejich využívání pouze pro ochranu či testování a nikdy k útoku.

- **Kali Linux** je linuxová distribuce postavená na distribuci Debian. Výhodou tohoto odvození z jiné distribuce je jednodušší vývoj a vydávání nových záplat, jelikož jsou sdílené s původní distribucí. Hlavním zaměřením této distribuce jsou penetrační testeři z důvodu nativního začlenění různých nástrojů pro analýzu a napadání počítačových sítí např. Wireshark, Ettercap, DNSChef atd. Další velkou výhodou je možnost provozovat Kali Linux z externího úložiště jako je USB flash disk, odpadá tím nutnost mít operační systém nainstalovaný fyzicky na laptopu nebo počítači. Narozdíl od ostatních podobných operačních systémů je pro tento provoz plně uzpůsoben a poskytuje plnou funkcionalitu závislou pouze na rychlosti použitého externího disku. Menší nevýhodou je snížený výkon kvůli pomalejšímu úložišti a neúplném přístupu hardware využívaného zařízení (27).
- **Wireshark** se využívá pro monitorování síťového prostředí. Není to sice nástroj, který se dá využít pro větší sítě, ale je vhodný pro analýzu během penetračního testování nebo pro běžné úkony vyžadující znalost síťového prostředí a jeho provoz. Nástroj funguje jako agent začleněný do sítě pomocí monitor protokolu. Jeho úkol je zachycovat všechny rámce, jež jsou v síti zasílány a přečíst je bez zásahu do jejich nesené informace. Dále je zapíše do logu, který ukládá pro možnost lepší analýzy (28).
- **Ettercap** je bezplatný a otevřený síťový bezpečnostní nástroj pro útoky typu „Man in the middle“ na vnitřní síť. Jeho výhodou je grafické uživatelské prostředí a velká škála

možných útoků, kterou nástroj nabízí. Taktéž kromě samotných útoku nabízí i prostředky pro analýzu sítě a získaných dat. Primární zaměření jsou bezpečnostní testeři. Jako vedlejší nežádoucí efekt je jeho využívání reálnými hackery pro napadání sítí (29).

- **Advanced IP Scanner** je další bezplatný nástroj. S jeho pomocí je možné skenovat zařízení přítomná v síti a získávat pomocí něho MAC a IP adresy. Pro získávání těchto adres program využívá packety ARP request (30).
- **Putty** je klient, který podporuje protokoly SSH, Telnet, rlogin a TCP. Dalším typem je připojení pomocí sériového portu, které je využíváno v rámci této práce. Klient je šířen pod volnou licencí (31).

2.9 První hypotéza

V případě první hypotézy je bráno v potaz, že s ohledem na velikost společnosti není možné udržovat všechna zapojená zařízení aktuální ze strany hardware a také ze strany firmware. Je to z důvodu vysokých nákladů, které musí být v jednu chvíli vynaloženy na výměnu a aktualizaci zařízení.

Přiřazování IP adres a VLAN za pomoci ANC funguje nejlépe na přepínačích Cisco řady Catalyst 2960 a jejich nástupcích Cisco Catalyst 9200L. V případě, kdy síť obsahuje některý ze starších modelů (Cisco Catalyst 3560, Cisco Catalyst 3570 atd.) může být funkcionalita omezena. Největší problém nastává, pokud je tento nepodporovaný přepínač nasazený jako řídící, a to z několika důvodů např. nižší výpočetní výkon, menší operační nebo vyrovnávací paměť atd. V těchto případech se může stát, že nastanou chyby nebo konflikty a VLANy jsou přiřazeny nesprávně nebo vůbec. To sice nemusí hned ukazovat na bezpečnostní problém, ale v případě častých výskytů těchto konfliktů se stává, že je nastavení portu změněno na statické, místo výměny přepínače pro zachování fungování technologie co nejlepší způsobem. Dotčené porty, které jsou nastaveny na statickou konfiguraci se bezpečnostním rizikem stát už mohou. A to v případě, kdy jsou porty na přepínači přepojeny. Může se stát, že jsou zařízení zapojena do portu se statickou konfigurací a tím je zařízení přiděleno do jiné VLANy. V tomto případě může docházet k narušení bezpečnosti.

2.9.1 Metodika testování první hypotézy

Metodika pro prokázání první hypotézy se zakládá na předělání infrastruktury, která bude postavena ze zastaralých zařízení představující centrum s nepodporovaným hardwarem.

V tomto případě se bude jednat o Clavister SG60 a řídící přepínač Cisco Catalyst 3560X-24T-S, jež se přestal prodávat v roce 2016, poslední aktualizace je pro něj plánována na říjen 2021. Jelikož je zařízení ještě podporované ze strany výrobce, není , nebezpečné, ale v tento moment by se mělo na centrech přestat vyskytovat. Kromě toho je postaveno na starší technologii procesoru a má menší flash paměť i paměť RAM. Pro nejpřesnější simulaci je vybaveno starším firmwarem, který se nejčastěji vyskytuje na těchto přepínačích v reálném provozu. Stejný případ nastává s i firewallem s takovým rozdílem, že poslední verze softwaru pro tento model vyšla v roce 2016. S touto výměnou bude vypomáhat síťový inženýr z firmy Dworkin spol. s r.o.

Po změně hardware a konfigurace bude probíhat samotné testování, které bude koncipováno jako postupné přepojování registrovaného zařízení do portů přepínače a zaznamenávání VLAN, které budou na porty dynamicky přiřazovány. Podle poměru správně a nesprávně přiřazených VLAN bude vyhodnoceno procento úspešnosti. Pokud bude adresa nesprávně přiřazena bude vyhodnoceno, zda šlo o nepřiřazení VLANy či přiřazení jiné VLANy. Zařízení, která budou připojována budou PC1 VLAN 600 a PC2 pro ověření obou virtuálních sítí. V závislosti na tomto výsledku se vyhodnotí závažnost bezpečnostního rizika. Pro co nejlépe měřitelný výsledek se provede těchto testů (zapojení) 50 pro různé porty rovnoměrně rozřazeny mezi PC1 a PC2, tedy 25 a 25 zapojení. Poté bude provedeno dalších 50 testů pro jeden port na přepínači a opět se testování rozdělí mezi zařízení PC1 PC2 rovným dílem. Důvod pro tento postup je eliminovat možné ovlivnění testu připojovaným zařízením a vylepšit tím test o jeho nezávislost.

2.9.2 Testování první hypotézy

Samotné testování probíhá ve dvou fázích. V každé fázi je vždy po odpojení a zapojení vypsána konfigurace konkrétního portu. Data z těchto výpisů jsou zapsány do tabulky pro přehledné srovnání a vyhodnocení. Nakonec je zařazena analýza každého ze scénářů a vyhodnoceno, jaké z výsledku plyne bezpečnostní riziko.

2.9.2.1 Náhodné zapojení (50 pokusů)

Porty na přepínači nastavené a připravené pro tento test jsou porty 7–23. Na těchto portech budou probíhat testy. Pořadí zapojování portů bude vygenerováno náhodně pomocí Excelového příkazu RANDBETWEEN (7;23). Tohle pořadí bude zachováno pro oba náhodné testy.

- **Měřený pokus (2 * 25 zapojení) náhodného portu** – pokud během testu nenastane žádná chyba VLANa pro PC1 by vždy měla být VLAN 600 a pro PC2 vždy VLAN 500. V případě jakékoli jiné hodnoty se bude jedna o chybu a bude zanalyzována jako závažná.

Tabulka 6: Náhodné zapojení PC1 a PC2.

	PC1			PC2		
Pokus	VLAN	Port	Chyba	VLAN	Port	Chyba
1	600	Gi/0/14	Ne	980	Gi/0/14	Ano
2	600	Gi/0/11	Ne	798	Gi/0/11	Ano
3	798	Gi/0/15	Ano	500	Gi/0/15	Ne
4	980	Gi/0/14	Ano	500	Gi/0/14	Ne
5	600	Gi/0/9	Ne	798	Gi/0/9	Ano
6	798	Gi/0/11	Ano	980	Gi/0/11	Ano
7	600	Gi/0/7	Ne	500	Gi/0/7	Ne
8	798	Gi/0/23	Ano	500	Gi/0/23	Ne
9	600	Gi/0/10	Ne	798	Gi/0/10	Ano
10	980	Gi/0/18	Ano	500	Gi/0/18	Ne
11	980	Gi/0/12	Ano	980	Gi/0/12	Ano
12	600	Gi/0/19	Ne	980	Gi/0/19	Ano
13	600	Gi/0/11	Ne	500	Gi/0/11	Ne
14	600	Gi/0/15	Ne	500	Gi/0/15	Ne
15	980	Gi/0/9	Ano	500	Gi/0/9	Ne
16	600	Gi/0/21	Ne	500	Gi/0/21	Ne
17	798	Gi/0/14	Ano	980	Gi/0/14	Ano
18	600	Gi/0/8	Ne	798	Gi/0/8	Ano
19	600	Gi/0/20	Ne	500	Gi/0/20	Ne
20	798	Gi/0/23	Ano	798	Gi/0/23	Ano
21	980	Gi/0/17	Ano	500	Gi/0/17	Ne
22	600	Gi/0/17	Ne	798	Gi/0/17	Ano
23	600	Gi/0/8	Ne	500	Gi/0/8	Ne
24	980	Gi/0/15	Ano	980	Gi/0/15	Ano
25	798	Gi/0/7	Ano	500	Gi/0/7	Ne

V tabulce 6 výše jsou vidět výsledky měření. Je možné pozorovat značnou nekonzistentnost. Při pohledu na nesprávná přiřazení není vidět na první pohled žádné pravidlo. Podle chování přepínače se dá vypozorovat nepředvídatelná chybovost. Při přiřazování se často

stává, že je přiřazena nesprávná VLANa. Pozitivním jevem je nepřiřazování VLAN jiných klientů, z toho vyplývá, že se nejedná o bezpečnostní hrozbu.

2.9.2.2 Testování jednotlivého portu (50 pokusů)

Pro druhou část testování byl vybrán náhodný port také pomocí excelového příkazu RANDBETWEEN (7;23). Pro tuto sadu testování vyšel port 10. Tento port bude využit pro testování obou počítačů.

- **Měřený pokus (2 * 25 zapojení) jednotlivého portu**

Tabulka 7: Zapojení do jednoho portu PC1 a PC2.

	PC1			PC2		
Pokus	VLAN	Port	Chyba	VLAN	Port	Chyba
1	798	Gi/0/10	Ano	500	Gi/0/10	Ne
2	798	Gi/0/10	Ano	500	Gi/0/10	Ne
3	798	Gi/0/10	Ano	500	Gi/0/10	Ne
4	798	Gi/0/10	Ano	500	Gi/0/10	Ne
5	980	Gi/0/10	Ano	980	Gi/0/10	Ano
6	600	Gi/0/10	Ne	980	Gi/0/10	Ano
7	600	Gi/0/10	Ne	980	Gi/0/10	Ano
8	600	Gi/0/10	Ne	980	Gi/0/10	Ano
9	600	Gi/0/10	Ne	980	Gi/0/10	Ano
10	600	Gi/0/10	Ne	980	Gi/0/10	Ano
11	600	Gi/0/10	Ne	980	Gi/0/10	Ano
12	600	Gi/0/10	Ne	980	Gi/0/10	Ano
13	600	Gi/0/10	Ne	500	Gi/0/10	Ne
14	600	Gi/0/10	Ne	500	Gi/0/10	Ne
15	600	Gi/0/10	Ne	500	Gi/0/10	Ne
16	600	Gi/0/10	Ne	500	Gi/0/10	Ne
17	600	Gi/0/10	Ne	500	Gi/0/10	Ne
18	600	Gi/0/10	Ne	500	Gi/0/10	Ne
19	600	Gi/0/10	Ne	500	Gi/0/10	Ne
20	600	Gi/0/10	Ne	500	Gi/0/10	Ne
21	600	Gi/0/10	Ne	500	Gi/0/10	Ne
22	600	Gi/0/10	Ne	500	Gi/0/10	Ne
23	600	Gi/0/10	Ne	500	Gi/0/10	Ne
24	600	Gi/0/10	Ne	500	Gi/0/10	Ne
25	600	Gi/0/10	Ne	500	Gi/0/10	Ne

Ve výsledcích druhé části měření, které jsou zaznamenané v tabulce 7 je vidět výrazně lepší výsledek, který ukazuje na lepší konzistentnost než v případě zapojování do náhodného portu. Při testu PC1 jsou sice ze začátku testu zaznamenány chyby, avšak dále jsou výsledky konzistentní. Ukazuje to na interní „učení“ přepínače. V druhém případě se tato chyba projevila až po prvních čtyřech úspěšných testech. To ukazuje spíše na chybu v komunikaci se serverem. Zařízení ovšem není odříznuto od internetu, pouze nemá přístup do VLANy 500.

2.9.3 Výsledek testů první hypotézy

Výsledky obou testů prokazují část hypotézy, a to takovou část, která mluví o konfliktu a přiřazení nesprávné VLANy. Část hypotézy, která se neprojevila je přiřazení VLANy jiného klienta. Z tohoto důvodu lze hypotézu z hlediska bezpečnosti považovat za bezpečnou.

V tabulce osm jsou zaznamenány počty chyb a jejich procento. V případě zapojování zařízení do náhodného portu je pravděpodobnost chyby 48% a navíc nelze vypozorovat pravidlo, podle kterého by se dala zvýšit úspěšnost. Naopak v případě jednotlivého portu je vidět, že po několika chybách se vždy problém napraví. Chybovost se zastavila na 26% a pro největší úspěšnost stačí zařízení zapojit několikrát po sobě. V testu se prokázalo, že po dostatečném počtu opakování se konfigurace propíše a VLANa je přiřazena v pořádku.

Tabulka 8: Počty chyb při zapojování.

	Počet chyb	Procento chyb
Počet chyb při testu náhodného portu	24	48%
Počet chyb při jednotlivého portu	13	26%
Součet chyb při zapojování	37	37%

Všechna měření, která proběhla v této hypotéze jsou zaznamenána v příloze II.

2.10 Druhá hypotéza

Druhá hypotéza je základem pro testování hypotézy třetí. Pokud nebude tato hypotéza úspěšná bylo by nutné pro hypotézu třetí nastavit umělé laboratorní podmínky, které ovšem neodpovídají reálnému prostředí společnosti. Základem pro úspěšnost celé metody je fyzický přístup k zařízením, která jsou zapojena do sítě. Tato skutečnost může nastat v případě, kdy si klient zapomene zamknout kancelář. Může nastat i situace, kdy nezamkne uklízecí služba

během večerního úklidu. Ta má přístup do všech kanceláří. př Předpokládá se, že v takovém případě přečte potřebné informace (MAC adresa) pomocí přenosného routeru nebo přímo ze štítku na zařízení (typicky stolní PC, Wi-Fi AP, tiskárny).

Tato hypotéza bere v potaz, že jsou tyto informace už známé. Pokus bude tedy pokračovat k dalším krokům, což je samotné napadení virtuální sítě. Jelikož je logika přiřazování VLAN a IP adres založeno na dynamickém přístupu, pro úspěšné napadení už pouze stačí najít aktivní port kdekoli na centru a připojit se do sítě. Útočník se dostane do zabezpečené sítě klienta v případě, že jsou všechny předpoklady správné.

Tato hypotéza bude testována na poslední verzi schváleného hardware a software pro provozování ANC, tím bude zajištěna konzistentnost výsledků a bude zamezeno chybám, které se objevují v hypotéze jedna.

2.10.1 Metodika testování druhé hypotézy

Základem pro druhou hypotézu je demonstrace toho , jakým způsobem pracuje přepínač s virtuálními sítěmi. Představení fungování bude probíhat připojením dvou zařízeních PC1 VLAN 600 a PC2, která jsou zaregistrované pod jiným klientem. A nadále demonstrováním logického oddělení obou zařízení. Bude dokázáno, že sítě nejsou nijak logicky propojeny a nemohou spolu tato zařízení komunikovat na lokální síti. Pro prokázání možnosti komunikace mezi zařízeními bude využito příkazu „ping“.

Po prokázání této skutečnosti bude u PC1 VLAN 600 změněna MAC adresa na PC1 VLAN 500. V tento moment by se mělo to stejné zařízení zařadit pod VLAN 500. Důkaz dané skutečnosti se prokáže možností komunikovat na lokální síti mezi zařízeními PC1 VLAN 500 a PC2. Pokud se tato skutečnost prokáže bude objevena závažná bezpečnostní trhlina, která dokáže výrazně ovlivnit datovou integritu klientů i společnosti.

Tento test bude proveden desetkrát, z důvodu prokazatelnosti. Testy jsou založeny na výše popsané metodice, kdy bude MAC adresa měněna z adresy pro VLAN 500 na adresu pro VLAN 600 a zpět 10-krát po sobě, při každé změně bude ověřeno přiřazení VLANy vypsáním konfigurace portu. Zkouška bude probíhat ve dvou sadách po deseti testech. Jedna sada bude probíhat pro zařízení zapojené do náhodného portu a druhá sada zapojení vždy do stejného portu.

2.10.2 Testování druhé hypotézy

Samotné testování bude probíhat v podobě demonstrace fungování virtuálních sítí a dále ve dvou oddělených pokusech.

První pokus se bude zabývat zapojováním zařízení do náhodného portu, tyto porty budou vybírány pomocí příkazu RANDBETWEEN (7;23) v programy Microsoft Excel.

Druhý pokus bude probíhat stejným způsobem jako první s rozdílem zapojování zařízení pouze do jednoho portu. Tento port bude vybrán příkazem RANDBETWEEN (7;23) opět v programu Microsoft Excel.

2.10.2.1 Demonstrace fungování virtuálních sítí

V demonstraci bude předvedeno, jakým způsobem rozdělují virtuální sítě lokální síť. Hlavním předpokladem je zařazení dvou zařízení do odlišných VLAN, jak je vidět ve výpisu konfigurace z přepínače na obrázcích 15 a 16.

```
SW00-01-01-2960.6748#sho mac address-table interface gigabitEthernet 1/0/22
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 600    00e0.4c68.1f91    DYNAMIC     Gi1/0/22
Total Mac Addresses for this criterion: 1
```

Obrázek 15: Přiřazení VLAN pro zařízení PC1.

```
SW00-01-01-2960.6748#sho mac address-table interface gigabitEthernet 1/0/21
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 500    1062.e517.095e    DYNAMIC     Gi1/0/21
Total Mac Addresses for this criterion: 1
```

Obrázek 16: Přiřazení VLAN pro zařízení PC2.

Dále jsou na obrázcích 17 a 18 vidět přiřazené IP adresy u PC1 A PC2 ve vlastních VLANách. Tato data jsou zjišťována pomocí programu Advanced IP Scanner, který prohledává zadaný rozsah a pomocí ARP request packetů zjistí svoje síťové okolí.

Status	Name	IP	Manufacturer	MAC address
	192.168.56.1	192.168.56.1	Clavister AB	40:84:93:15:B3:25
	PC1	192.168.56.20	Hewlett Packard	00:E0:4C:68:1F:91

Obrázek 17: Wireshark – IP PC1.

Status	Name	IP	Manufacturer	MAC address
	192.168.55.1	192.168.55.1	Clavister AB	40:84:93:15:B3:25
	PC2	192.168.55.20	Hewlett Packard	10:62:E5:17:09:5E

Obrázek 18: Wireshark – IP PC2.

Na obrázcích 19 a 20 je pomocí příkazové řádky Microsoft Windows zobrazeno, že jedno zařízení není schopné komunikovat s druhým a naopak. Tento fakt je dokazatelný za pomocí příkazu Ping, který je využíván pro zjištění odezvy připojené mezi jednotlivými uzly sítě. V tomto případě je jedná o PC1 A PC2. Výsledkem těchto testů je 100% ztráta packetů, to znamená nemožnost vzájemné komunikace.

```
C:\Users\PC2>ping 192.168.56.20

Pinging 192.168.56.20 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.56.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Obrázek 19: Ping PC1 z PC2.

```
C:\Users\PC1>ping 192.168.55.21

Pinging 192.168.55.21 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.55.21:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Obrázek 20: Ping PC2 z PC1.

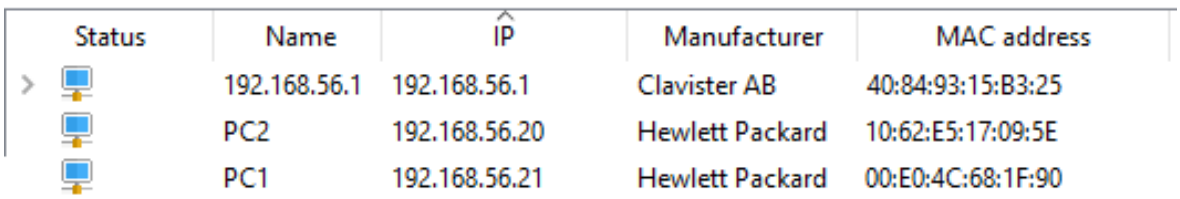
2.10.2.2 Testování náhodného zapojení (10 testů)

Ve výsledcích prvního testu s náhodným zapojováním je vidět, že konzistentnost přiřazování VLAN je 100%, což potvrzuje funkčnost ANC na podporovaném hardwaru a softwaru. Dále také potvrzuje hypotézu a ukazuje, že je možné zařadit jedno zařízení, které umožňuje měnit MAC adresu do více VLAN a tím se dostat do virtuální sítě bez nutnosti projít registrací adresy pod tohoto klienta. Ukazuje to na bezpečnostní trhlinu v systému ANC, která při dostatečné znalosti sítě a této technologie dovoluje poměrně jednoduše napadnout cizí virtuální sítě a případně se z ní snažit ukrást data.

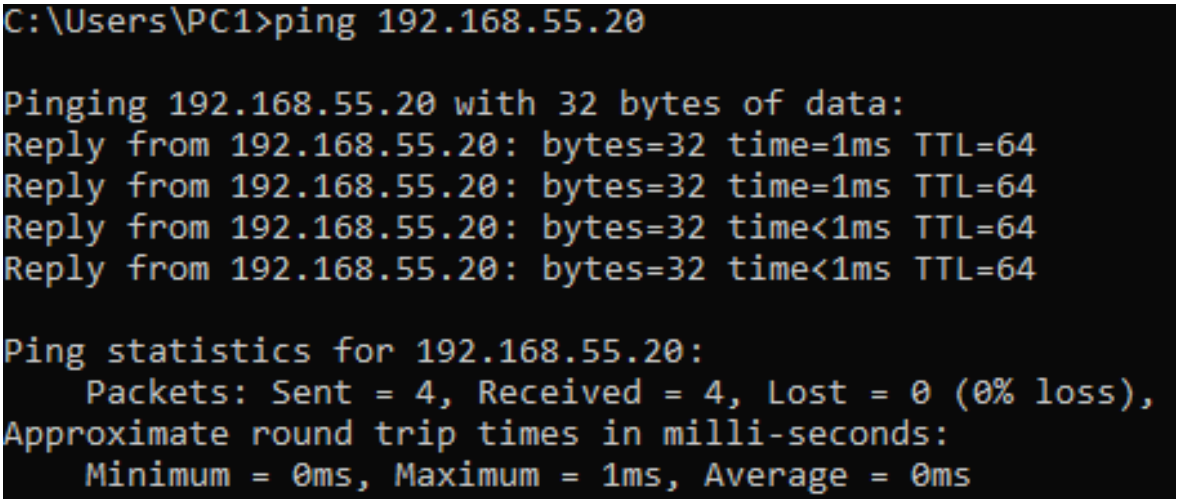
Tabulka 9: Testování náhodného zapojení.

	PC1 – VLAN 600			PC1 – VLAN 500		
Pokus	VLAN	Port	Chyba	VLAN	Port	Chyba
1	600	Gi/0/20	Ne	500	Gi/0/20	Ne
2	600	Gi/0/11	Ne	500	Gi/0/11	Ne
3	600	Gi/0/22	Ne	500	Gi/0/22	Ne
4	600	Gi/0/17	Ne	500	Gi/0/17	Ne
5	600	Gi/0/12	Ne	500	Gi/0/12	Ne
6	600	Gi/0/15	Ne	500	Gi/0/15	Ne
7	600	Gi/0/10	Ne	500	Gi/0/10	Ne
8	600	Gi/0/17	Ne	500	Gi/0/17	Ne
9	600	Gi/0/17	Ne	500	Gi/0/17	Ne
10	600	Gi/0/10	Ne	500	Gi/0/10	Ne

Obrázek 21 ukazuje úspěšné zařazení PC1 do VLANy 500. Tento jev dokazuje možnost přesunování zařízení mezi VLANami bez nutnosti přeregistrování. Dále je na obrázku 22 vidět příkaz ping, který probíhá s 0% ztrátou packetů. To dokazuje možnost komunikace mezi PC1 a PC2 v rámci VLANy 500.



Obrázek 21: Wireshark PC1 a PC2 ve stejné síti.



Obrázek 22: Kontrola možnosti komunikovat mezi PC1 a PC2.

2.10.2.3 Testování jednotlivého portu (10 testů)

Testování jednotlivého portu prokázalo stejný výsledek jako testování náhodného portu. Na výsledku se tedy nic nemění, pouze se potvrzuje výstup z předchozího testu. Výsledky tohoto testování jsou zaznamenány v tabulce 10.

Tabulka 10: Testování jednotlivého portu.

	PC1 – VLAN 600			PC1 – VLAN 500		
Pokus	VLAN	Port	Chyba	VLAN	Port	Chyba
1	600	Gi/0/21	Ne	500	Gi/0/21	Ne
2	600	Gi/0/21	Ne	500	Gi/0/21	Ne
3	600	Gi/0/21	Ne	500	Gi/0/21	Ne
4	600	Gi/0/21	Ne	500	Gi/0/21	Ne
5	600	Gi/0/21	Ne	500	Gi/0/21	Ne
6	600	Gi/0/21	Ne	500	Gi/0/21	Ne
7	600	Gi/0/21	Ne	500	Gi/0/21	Ne
8	600	Gi/0/21	Ne	500	Gi/0/21	Ne
9	600	Gi/0/21	Ne	500	Gi/0/21	Ne
10	600	Gi/0/21	Ne	500	Gi/0/21	Ne

Pro úplné ověření byl proveden i test přítomnosti PC1 a PC2 ve stejné VLANě. Na obrázku 23 můžeme vidět přiřazení IP adresy ve stejném IP rozsahu. Na obrázku 24 je prokázána možnost komunikace mezi zařízeními v této VLANě pomocí příkazu ping s 0% ztrátou packetů.

Status	Name	IP	Manufacturer	MAC address
	192.168.55.1	192.168.55.1	Clavister AB	40:84:93:15:B3:25
	PC2	192.168.55.20	Hewlett Packard	10:62:E5:17:09:5E
	PC1	192.168.55.21	Hewlett Packard	00:E0:4C:68:1F:90

Obrázek 23: Wireshark PC1 a PC2 ve stejné síti.

```
C:\Users\PC1>ping 192.168.55.20

Pinging 192.168.55.20 with 32 bytes of data:
Reply from 192.168.55.20: bytes=32 time=1ms TTL=64
Reply from 192.168.55.20: bytes=32 time<1ms TTL=64
Reply from 192.168.55.20: bytes=32 time<1ms TTL=64
Reply from 192.168.55.20: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.55.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Obrázek 24: Kontrola možnosti komunikovat mezi PC1 a PC2.

2.10.3 Výsledky testování druhé hypotézy

V případě druhé hypotézy byla prokázána možnost připojení do sítě zařízení, které se dokáže vydávat za zařízení přiřazeno do existující virtuální sítě klienta a tím tuto síť napadnout a případně způsobit únik dat. Tohle zjištění ukazuje na nízký stupeň zabezpečení použitého řešení a nutnost zavedení dalších možností ověření, která jsou do sítě připojována.

Navíc nelze výsledek považovat za chybu přiřazení nebo konflikt při přiřazování VLAN, jelikož byla tato bezpečnostní trhlina prokázána ve dvou nezávislých testech, které navíc proběhly bez zaznamenání jedné chyby. Z toho vyplívá, že pokus probíhal přesně podle předpokladů představených v hypotéze.

Díky tomuto výsledku je možné přistoupit k hypotéze tři bez nutnosti vytvářet laboratorní prostředí a otestovat ji přímo se současným nastavením sítě.

Všechna měření, která proběhla v této hypotéze jsou zaznamenána v příloze III.

2.11 Třetí hypotéza

Třetí hypotéza těží z úspěšnosti druhé hypotézy a počítá s aktivním napadnutím sítě (ARP spoofing, ARP poisoning) a následnou analýzou zajištěných dat. Zatím není známo, jestli bude možné pomocí těchto technik dosáhnout výsledku, jelikož není známá úroveň zabezpečení a ochrana počítačové sítě. Účel tohoto útoku je získání a možnost monitoringu packetů odesílaných napadeným zařízením. Důvod, proč tento test závisí na úspěchu druhé hypotézy je nemožnost napadnutí sítě, které není účastník přímo členem. V případě, kdyby byl do této sítě začleněn (v druhé hypotéze) může útočník přejít k útoku na ostatní členy sítě.

2.11.1 Metodika testování třetí hypotézy

Základem této metodiky bude zapojení tří počítačů do sítě a do stejné VLANy. V tomto případě se bude jednat o PC1 V500, PC2 a PC3. Celý proces bude probíhat ve VLANě 500, která byla vybrána jako virtuální síť k napadnutí. PC1 bude vystupovat jako zařízení nabourávající síť a pokoušející se o narušení bezpečnosti a případnou krádež dat. PC2 zde vystupuje jako běžný uživatel a v tomto případě oběť případného útoku. PC3 je v síti zařazen jako pasivní uživatel a jeho úkolem bude zaznamenávání a analýza dat.

Průběh útoku bude probíhat následovně. Útočník PC1, který je vybaven operačním systémem Kali Linux a nástrojem Ettercap začne do sítě vysílat dotazy ARP requst pro zmapování sítě a zajištění MAC adres okolních zařízení. Ze strany sítě ovšem stále působí jako běžný klient. Na PC3 je spuštěný nástroj Wireshark, který síť monitoruje. V tento moment se začíná ukazovat co se v sítí děje.

Po zmapování sítě je útočníkovi známá MAC adresa oběti a začíná útok ARP spoofing. Tento útok probíhá přesměrováním všeho síťového provozu oběti přes síťové rozhraní útočníka. Pokud je zabezpečení sítě nastaveno správně, mělo by velmi rychle dojít k zablokování všech vysílaných dotazů. Pokud se tak nestane uvidíme monitorovacím PC3 probíhající útok a PC1 budeme schopni odposlouchávat síťovou komunikaci. V tomto případě to pro testování znamená objevení velmi závažné bezpečnostní trhliny a nutnost vytvoření bezpečnostní záplaty.

2.11.2 Testování třetí hypotézy

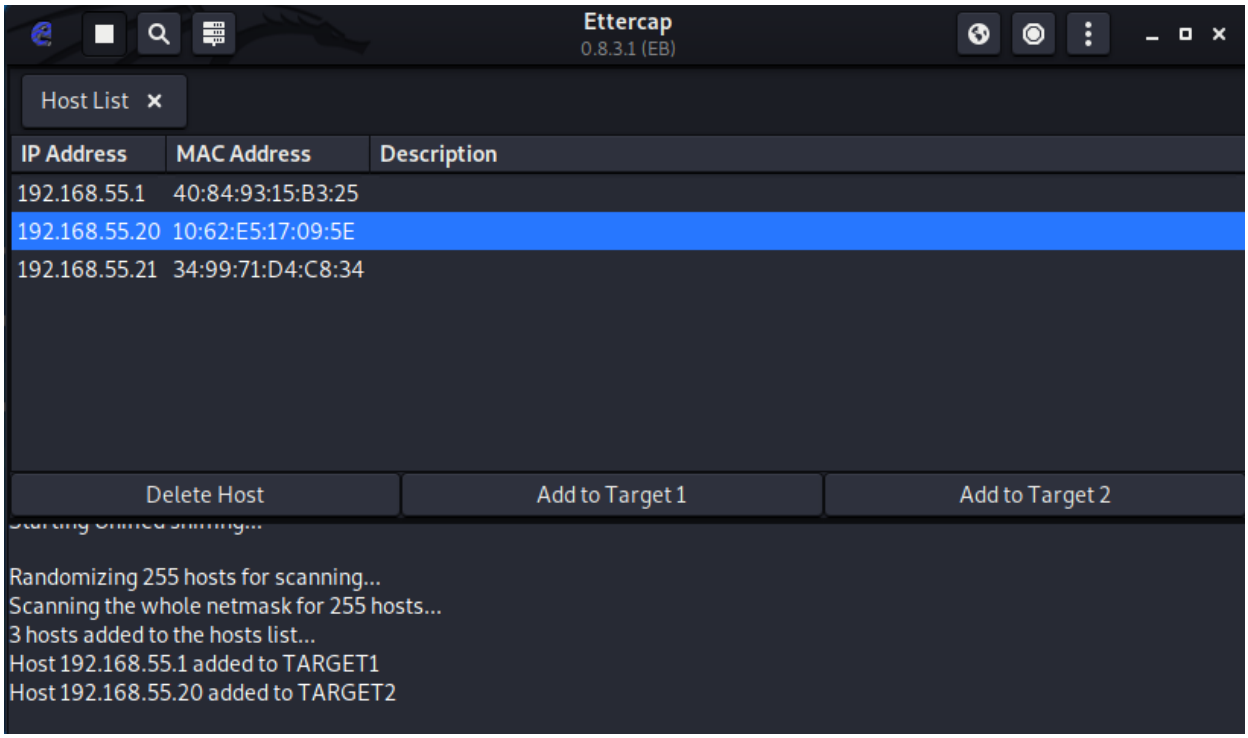
Po úspěšném napadnutí VLANy v hypotéze dvě je dalším úkolem se pokusit vysledovat komunikaci mezi vybranou obětí a veřejným internetem. V této demonstraci nepůjde přímo

o interpretaci vysledovaných dat, ale demonstrování možnosti zaútočit na síť. To představuje velmi vážnou bezpečnostní trhlinu, která není pro síť s podobným zaměřením a parametry přípustná.

2.11.2.1 Napadnutí sítě programem Ettercap

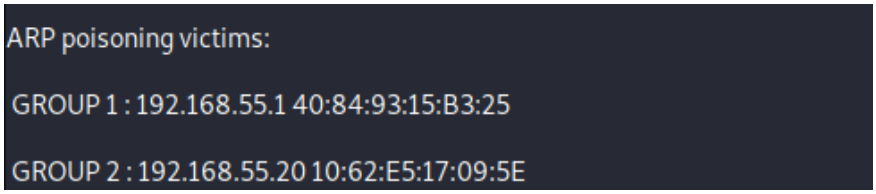
Jelikož je program Ettercap grafický, je vysvětlení jeho používání poměrně jednoduché. Na obrázku 15 je vidět rozhraní po přidání cílů pro útok. Pod cílem 1 (Target1), je přiřazeno zařízení s MAC adresou 40:84:93:15:B3:25, což je výchozí brána celé virtuální sítě. Z fyzického hlediska je to firewall Clavister E80. Druhé zařízení, které je přiřazeno jako cíl 2 (Traget2) je cílem tohoto útoku. Jedná se o zařízení PC2 a jeho dynamicky přiřazená IP adresa je 10:62:E5:19:09:5E. Zařízení, které vystupuje jako útočník je PC1 s MAC adresou 00:E0:4C:68:1F:90.

Po vybrání těchto zařízení je zahájen útok, a to konkrétně ARP poisoning. Tento útok typu Man in the Middle útočí na prostor mezi zařízením a výchozí bránou a snaží se zachytávat komunikaci, která tímto prostorem prochází. Pomocí podobných útoků je možné ukrást přihlašovací jména a hesla.



Obrázek 25: Prostředí nástroje Ettercap.

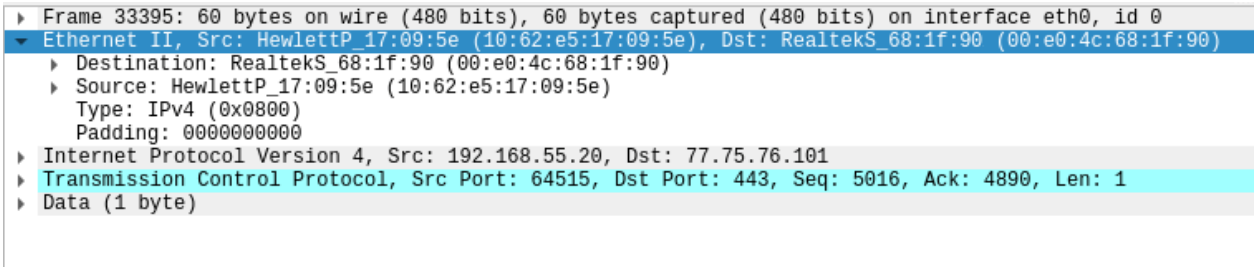
Po tomto nastavení je zahájen útok. Pro prokázání úspěšnosti tohoto útoku bude v další kapitole využit nástroj Wireshark využívající monitoraci sítě a vyhodnocení, zda probíhající útok probíhá.



Obrázek 26: Zahájení útoku ARP poisoning.

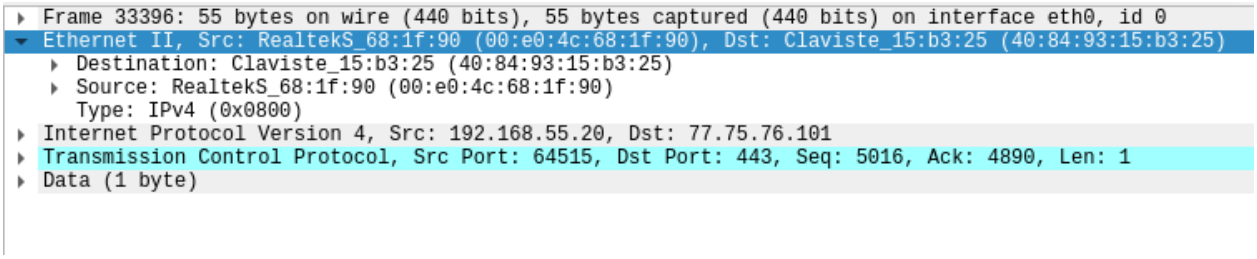
2.11.2.2 Monitorování pomocí programu Wireshark

Po zahájení útoku nastupuje část, ve které probíhá monitorování útoku a zjištění, jestli je síť schopná útoku odolat či ho zastavit. Obrázek 27 zobrazuje výpis rámce, který byl zachycen a je na něm jasně vidět, že zdroj tohoto rámce je zařízení PC2 s MAC adresou 10:62:E5:19:09:5E. To je zařízení, které bylo vybráno jako zařízení pro napadnutí. V detailu rámce je vidět destinace tohoto rámce, kterou je IP adresa 77.75.76.101, což je adresa z bloku adres vlastněná společností Seznam.cz. Tohle dokazuje, že se jedná o odchozí rámec, který by měl procházet přes výchozí bránu. I přesto je v rámci jako destinace v lokální síti zařazeno zařízení s MAC adresou 00:E0:4C:68:1F:90, což je zařízení PC1 neboli útočník.



Obrázek 27:Wireshark přesměrování provozu zdroj.

Obrázek 28 ukazuje druhou část řetězce a to, jakým způsobem komunikuje útočník s výchozí bránou virtuální sítě. Jako konečná destinace je stále společnost Seznam.cz, ale jako zdroj je zde PC1, což je útočník. Destinace v lokální síti je tentokrát už opravdová výchozí brána, která rámec převezme a přepošle do internetu.



Obrázek 28: Wireshark přesměrování provozu destinace.

2.11.3 Výsledky testování třetí hypotézy

V průběhu testu třetí hypotézy byla prokázána možnost napadnutí virtuální sítě pomocí útoku ARP poisoning. Tento výsledek představuje velkou bezpečnostní trhlinu, která v propojení s výsledkem hypotézy dvě představuje potenciální bezpečnostní incident.

Tento výsledek ukazuje, že útok byl úspěšný. Útočník bych schopen svojí aktivitou změnit ARP tabulku oběti a tím se vydávat za výchozí bránu lokální sítě pro napadené zařízení. Díky zaměření útoku pouze na jedno zařízení není síť zahlcena více ARP reply packety a detekce je mnohem složitější.

2.12 Analýza finančních rizik

Analýza finančních rizik se bude zaměřovat na region Velké Británie a na potenciální finanční poškození. To může vzniknout kvůli úniku dat. Klienti využívají infrastrukturu firmy, a proto je v případě úniku společnost zodpovědná za bezpečnost těchto dat a s tím spojené případné finanční postihy Údaje ohledně pokut jsou pro tuto analýzu vypočítány jako střední hodnota, kterou je možné vymáhat v rámci zákonu o ochraně dat. Tato hodnota je 17,5 milionu liber. Z tohoto důvodu bude uvažováno o hodnotě 10 milionu liber v případě bezpečnostního incidentu (32).

2.12.1 Identifikace a hodnocení rizik

Tabulka číslo jedenáct hodnotí pravděpodobnost, kdy nastanou jednotlivá rizika a rozdělují ji na škále od 1 do 10. Tato škála se pohybuje od téměř žádné pravděpodobnosti až po vysokou.

Dále hodnotí dopad také na škále od 1 do 10, kdy se dopad pohybuje od minimálního po kritický.

Tabulka 11: Ohodnocení rizik.

Pravděpodobnost	Dopad
Téměř žádná: 1-2 (0 %-19 %) Nízká: 3-4 (20 %-39 %) Pravděpodobná: 5-6 (40 %-59 %) Více pravděpodobná: 7-8 (60 %-79 %) Vysoká pravděpodobnost: 9-10 (80 %-100 %)	Minimální:1-2 Méně významný: 3-4 Významný: 5-6 Velmi významný: 7-8 Kritický: 9-10

Identifikace a hodnocení rizik pro projekt je zaneseno v tabulce 12. . Zaměřuje se pouze na rizika související s touto diplomovou prací. Tedy s nebezpečím , které by pro společnost mohlo nést nečekané finanční náklady.

Tabulka 12: Identifikace a hodnocení rizik.

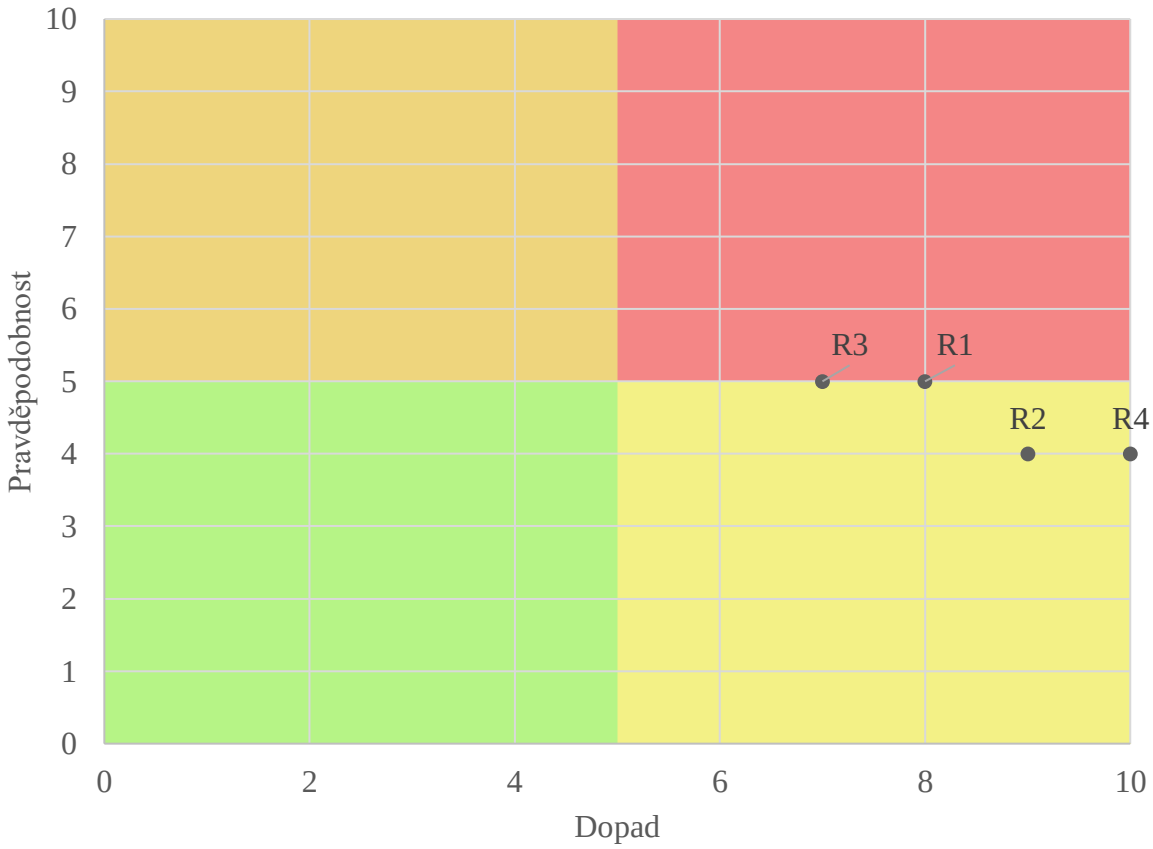
Riziko	Hrozba	Scénář	Pravděpodobnost	Dopad	Hodnota rizika
R1	Napadnutí virtuální sítě klienta	Útočník se naboural do virtuální sítě klienta	5	8	40
R2	Únik dat klienta	Po nabourání do virtuální sítě nastane únik dat	4	9	36
R3	Nabourání do virtuální sítě společnosti	Útočník se naboural do virtuální sítě společnosti	5	7	35
R4	Únik dat společnosti	Po nabourání do virtuální sítě společnosti nastane únik dat o klientech	4	10	40

2.12.2 Mapa rizik před zavedením opatření

Graf tři zobrazuje mapu rizik, která ovlivňují projekt před zavedením opatření a dále také ukazuje na vážnost jednotlivých rizik.

Graf je rozdělen na čtyři obdélníky:

- **Zelený obdélník** – bezvýznamná rizika – není nutné opatřovat, zle podstoupit.
- **Žlutý obdélník** – běžná rizika – opatřením jde většinou eliminovat.
- **Oranžový obdélník** – významná rizika –je nutné řešit zavedením opatření, většinou nejde eliminovat pouze snížit.
- **Červený obdélník** – kritická rizika – je nutné řešit zavedením opatření, jsou to velká rizika



Graf 3: Mapa rizik před zavedením opatření.

Distribuce rizik tohoto projektu je poměrně jednostranná. Na grafu se nachází ve žlutém a na rozmezí žlutého a červeného obdélníku. Jsou to běžná rizika, která se dají zmírnit aplikováním opatření. Dále se dvě rizika nachází na rozmezí červeného a žlutého čtverce. Na tato nebezpečí bude nahlíženo jako na kritické. Bude u nich nutné aplikovat opatření, aby bylo riziko pro společnost přijatelné.

2.12.3 Opatření

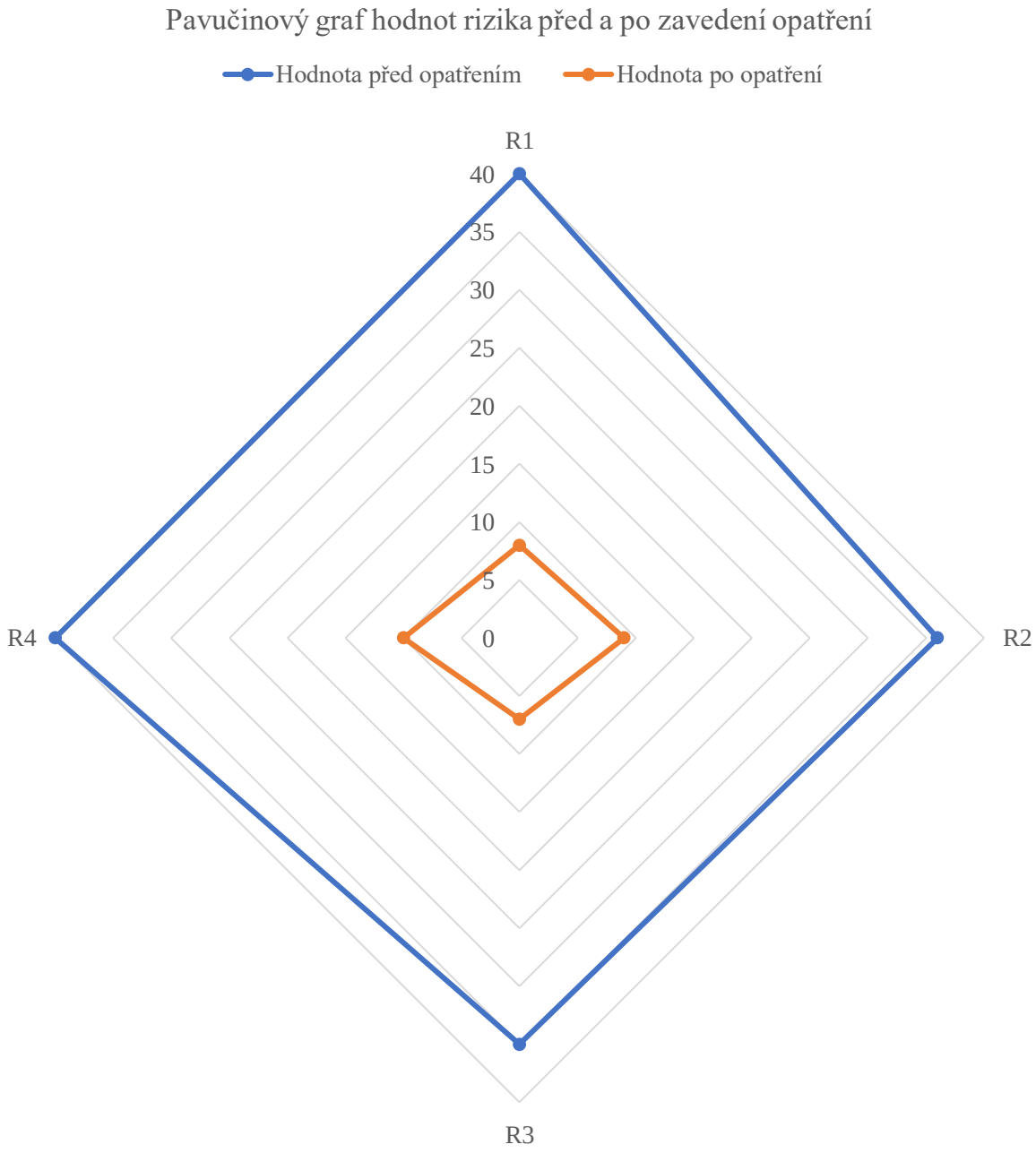
V tabulce níže je zobrazeno zavedení opatření k dříve nalezeným rizikům. Ta změní hodnoty jednotlivých rizik na nové přijatelné hodnoty. Přijatelná úroveň rizika je taková, kterou se společnost rozhodne podstoupit a je ochotna čelit následkům v případě potřeby.

Tabulka 13: Tabulka aplikace opatření pro snížení rizik.

Původní hodnoty					Nové hodnoty			
Riziko	Hrozba	Pravděpodobnost	Dopad	Hodnota rizika	Opatření	Pravděpodobnost	Dopad	Hodnota rizika
R1	Napadnutí virtuální sítě klienta	5	8	40	Zavést vícefázové ověření zařízení při připojení do sítě	1	8	8
R2	Únik dat klienta	4	9	36	Zavedení aktivní analýzy síťového prostředí pro zabránění útokům	1	9	9
R3	Nabourání do virtuální sítě společnosti	5	7	35	Zavést vícefázové ověření zařízení při připojení do sítě	1	7	7
R4	Únik dat společnosti	4	10	40	Zavedení aktivní analýzy síťového prostředí pro zabránění útokům	1	10	10

2.12.4 Pavučinový graf hodnot rizika před a po zavedení opatření

Mapa rizik po zavedení opatření je zobrazena pomocí pavučinového grafu. Je jasně vidět, že opatření zabrala a snížila riziko. Dále se práce věnuje opatřením v třetí části práce.



Graf 4: Pavučinový graf hodnot rizika před a po zavedení opatření.

3 Návrh vlastního řešení

Kapitola návrhu vlastního řešení se zabývá rozpracováním analyzovaných problémů v druhé kapitole. Snaží se dát všechny zjištěné nedostatky do kontextu s reálným stavem a navrhnout cestu pro zlepšení současné situace. První kapitola se věnuje hypotéze jedna, která sice prokázala chybovost, ale není nebezpečná. V případě hypotézy dvě a tři se v průběhu testování objevily vážné bezpečnostní trhliny. Návrhům na zlepšení těchto problémů se věnují kapitoly dvě a tři. Poslední kapitola se zabývá ekonomickým zhodnocením celkového řešení, které by bylo nutné podniknout pro zamezení případným bezpečnostním incidentům a z nich plynoucích ekonomických dopadů.

3.1 Návrh řešení první hypotézy

Jelikož se chybné přidělení VLAN projevilo v průběhu obou testů a s oběma zařízeními, můžeme předpokládat, že chyba je na straně sítě, a ne na straně připojovaných zařízení. Pozitivním výsledkem vycházejícím z tohoto testu je to, že sice přiřazování neprobíhá správně a zařízení nejsou v některých případech zařazena do správné VLANy, ale vždy byla zařazena do VLANy 980 nebo 798. Sice to není správný výsledek, ale kromě komplikací pro klienta, který se může setkat s obtížemi s přiřazením správné sítě se nejedná o bezpečnostní hrozbu, což je pro tuto práci důležité. Pokud je zařízení zařazeno do VLANy 980 a je mu dán přistup do internetu, e mu odepřena komunikace se všemi ostatními zařízeními v síti. To byl nejčastější výsledek, který testu vyšel. Druhá možnost výsledku VLAN 798 je síť, která se nijak neliší od VLANy 980 s jediným rozdílem a to takovým , že zařízení nemá přistup do internetu.

Konkrétně v těchto případech se jedná o problémy způsobené většinou kombinací zastaralého softwaru a hardwaru. Část problémů se dá řešit pouze aktualizací softwaru, což je z hlediska zajištění podpory mnohem jednodušší a levnější proces než výměna všech zařízení za nové. Pokud se řešení zaměří na konkrétní množství zařízení, která se v současné době nachází na centrech a bylo by je nutné vyměnit nebo aktualizovat, jdou tyto počty do stovek až tisíců kusů. Pro lepší představu se v Evropě v současné době nachází okolo 1 300 center a na zhruba 850 centrech je minimálně jedno nepodporované

zařízení. Tato data jsou společnosti dostupná z jejich interních systémů a pravidelného reportu, který se generuje každý týden. Z pohledu celého světa, kde je těchto center dohromady asi 3 400, se dá předpokládat stejný podíl neaktuálních zařízení.

3.1.1 Řešení problému se softwarem

Aktualizace softwaru zařízení sice neřeší tento problém úplně, ale alespoň jej utlumuje do únosné míry. Z důvodu obrovského množství zařízení, která je potřeba aktualizovat, není možné provézt aktualizace všech v jeden moment. Proto by bylo vhodné provádět aktualizace pravidelně při údržbě síťové infrastruktury centra, která probíhá každé 3 měsíce. V současné době se při údržbě jedná pouze o kontrolu správného nastavení základních zařízení jako jsou firewally a řídící přepínače. Součástí této údržby není aktualizace softwaru.

Pro ušetření nákladů a co nejrychlejší distribuci aktualizací by bylo nejvhodnější kontrolovat aktuálnost softwarového vybavení v průběhu pravidelné údržby. Výhodou tohoto postupu je snížení nákladů na výjezd technika. Jelikož údržba probíhá pravidelně stačí přidat tuto položku do agenty údržby bez přidaných nákladů.

3.1.2 Řešení problému s hardwarem

Plné vyřešení problému je teprve tehdy, když je zastaralé zařízení vyměněné za podporované. Tato společnost má poměrně velké množství hardwaru, který byl navrácen do inventáře po zavření starších center. Díky tomuto inventáři podporovaných zařízení je možné snížit náklady na výměnu. Navíc je možné zkombinovat výměnu přepínačů a firewallů a vyměnit tato zařízení během běžné návštěvy technika. Tím se sníží případné dodatečné náklady na co nejnižší možnou míru. Pro případy, na které by nevystačily použité zařízení anebo by musel být naplánován výjezd technika mimo běžné návštěvy, bude nutné zaplatit zařízení nové a započítat i výjezd technika. Průměrná cena nového zařízení je 600 liber a výjezd 250 liber. Nejedná se o přímé ohrožení bezpečnosti, takže budou náklady na výměnu zařízení sloužit pouze jako doporučení pro zlepšení funkčnosti sítě a spokojenosti zákazníků. Budou ovšem započítány do celkových nákladů ve finančním zhodnocení práce. Jelikož není známý počet zařízení, která se dají použít

z inventáře společnosti, bude cena za výměnu a výjezd technika vždy počítána v plné míře.

3.2 Návrh řešení druhé hypotézy

V průběhu druhé hypotézy bylo prokázáno, že je pomocí změny MAC adresy u zařízení možné infiltrovat VLANu, která mu není primárně přiřazena. Tento problém lze vyřešit několika způsoby, jejichž implementace by většinou znamenala zrušit nebo omezit funkčnost technologie ANC. Řešení bude zaměřeno na zachování plné funkčnosti tohoto systému. V tomto případě se tu nabízí možnost zavedení víceúrovňového ověření při přiřazování VLANy nově připojeného zařízení. Tento postup není možné aplikovat pro jednodušší zařízení bez pokročilejšího operačního systému. Z toho důvodu bude řešení rozděleno na dvě části. První část se bude věnovat zařízením s pokročilým operačním systémem a druhá jednodušším zařízením jako jsou tiskárny, přístupové body atd.

3.2.1 Řešení pro zařízení s operačním systémem

V tomto případě bude řešení založeno na vícefázovém ověření uživatele a zařízení. Proto se nabízí několik možných způsobů řešení. Důležitým předpokladem pro použití tohoto východiska je možnost použít jej na všech platformách. V současné době je možné zakoupit hotové řešení jako jsou šifrovací klíče v podobě USB klíčenek, systémy pro ověření pomocí SMS, emailu nebo různé autorizační aplikace od společnosti jako je Google nebo Microsoft. V ideálním případě by bylo vhodné implementovat více vrstev těchto ověřovacích systému. Je nutné, aby tohle ověřování probíhalo pouze u klientů, kteří využívají služeb privátní VLANy a to pouze v případě, že je zařízení odpojeno a je nutné změnit VLANu na portu, není těchto případů mnoho. Pro klienty, kteří využívají notebooků a každý den je do sítě připojují, bude nutné tohle ověření podstupovat při každém přepojení.

Protože je ve společnosti již v provozu masivní informační systém, dávalo by největší smysl vytvořit autentifikační systém, který by s tím současným byl kompatibilní nebo na míru vytvořený. V tomto případě připadají v úvahu dvě možnosti. Jedna z nich je Microsoft Authenticator, který by dokázal navázat na již spuštěné služby. To by ale

znamenalo nutit klienty k vytvoření účtu Microsoft a jelikož část klientů tyto služby nepoužívá mohlo by to pro ně znamenat nepohodlí a nepříjemnosti. Z tohoto důvodu by bylo lepší vytvořit řešení na míru.

Řešení na míru může být poměrně nákladný způsob, ale protože má tato společnost svoje vlastní vývojové oddělení, není nutné najímat externího dodavatele. Tohle má svoje výhody i nevýhody. Hlavní výhodou jsou nulové náklady na vývoj, možnost vnitřního řízení a v případě potřeby jednodušší zařazení změn během vývoje systému. Nevýhodou může být pomalejší vývoj v důsledku nutnosti se věnovat vývoji a podpoře i ostatních systémů a produktů, které pod tento tým spadají.

Z hlediska podoby tohoto systému není nutné řešit zařízení, která se připojují pouze pomocí bezdrátové sítě, jelikož se není v současné chvíli možné pomocí ní připojit do virtuálních síti klienta. Z tohoto důvodu je nutné vytvořit řešení, které bude fungovat na všech operačních systémech. Tyto systémy jsou Windows, MACOS, Chrome OS, iPadOS a Linux. Díky širokému portfoliu systémů, které je nutné podporovat se jako nejlepší způsob autentifikace jeví využít portálu ve webovém prohlížeči. Do tohoto portálu by se každý klient přihlásil svým vlastním účtem založeným v systému společnosti. Pro samotné ověření by bylo nejlepší využít zaslání ověřovacího kódu pomocí SMS nebo emailu. Z důvodu větší bezpečnosti je lepší využívat SMS, jelikož je mnohem složitější ji zachytnout nebo vysledovat. Dále se zde nabízí možnost ověření totožnosti klienta za pomoci skenu obličeje či prstu, jelikož je čím dál běžnější mít v laptopech, tabletech a podobných zařízeních možnosti biometrického ověření. V tom případě se přidává další vrstva zabezpečení, kterou je velmi těžké prolomit. S těmito požadavky je také nutné doplnit databázi uživatelských účtů o možnost přidávat další možnosti zabezpečení kromě hesla. Navíc je opět nutné vzít v potaz různé platformy. U počítačů s Windows je to Windows Hello, u Apple zařízení Touch ID nebo Face ID a u zařízení s Chrome OS se jedná o Biometric API.

Po úspěšném ověření klienta by se překontrolovala MAC adresa připojeného zařízení se zařízeními, která jsou registrována pod tímto účtem a v případě shody by byla přiřazena IP adresa a příslušná VLANa.

Další důležitou částí implementace nového systému je přizpůsobení původních pravidel pro připojování klientských zařízení do sítě s vlastní virtuální sítí. V tomto případě by bylo vhodné smluvně podchytit povinnost klientů chránit si svoji vlastní

virtuální sít minimálně dvoufázovou autentifikací pro všechny uživatele přistupující do této sítě. V případě, kdyby došlo k úniku dat, neměl by klient možnost nárokovat si odškodné z důvodu nesplnění podmínek nastavených poskytovatelem služeb.

3.2.2 Řešení pro zařízení bez operačního systému

V moment , kdy je do sítě s přiřazenou VLANou potřeba přidat zařízení, které nemá možnost otevření prohlížeče pro možnost ověření, jedná se o zařízení jako jsou tiskárny, routery, reproduktory atd. Pak je navrhované řešení povinnost nastavit IP adresu zařízení jako statickou a vyjmout ji z rozsahu DHCP. Takto se zajistí, že adresa nebude přiřazená žádnému jinému zařízení, které si o ni vyloženě neřekne.

Dalším mechanismem, který zajistí nemožnost napadení VLANy přes tuto MAC adresu je navázání MAC adresy na přiřazenou unikátní statickou IP adresu. To zajistí, že každé zařízení, které se připojí s touto MAC adresou a nebude mít IP adresu nastavenou staticky, nedostane žádnou adresu.

V případě, kdy by došlo k zjištění statické IP adresy, například po vytisknutí konfiguračního soboru tiskárny je tu další návrh pro zvýšení bezpečnosti a v případě pokusu o napadení znemožnění funkčnosti připojeného zařízení pomocí filtrace portů. Tím není myšleno filtrování fyzických portů, ale UDP portů. Pomocí nich jde povolit připojeném zařízení komunikovat pouze v určitém rozsahu. To znamená, že tiskárna bude moct pouze přijímat tiskové úlohy, odesílat naskenované dokumenty a zkontrolovat si případnou aktualizaci na serveru. Díky tomu bude zaručena nemožnost fungování mimo sítí povolené limity. V případě pokusu o napadení nebude možné v tomto pokračovat díky logickým omezením ze stran síťového prostředí.

Výhodou tohoto řešení je vysoká bezpečnost a nulové náklady na zavedení. Uvedení těchto pravidel do provozu vyžaduje pouze úpravu pravidel, podle kterých se klienti musí řídit. Pro donucení klientů dodržovat tyto pravidla je tu možnost smluvně podmínit nutnost mít podobná zařízení nastavená navrhovaným způsobem. Pro případ, kdy se stane jinak, může být odmítnuto vyplacení odškodnění z důvodu nedodržení interních předpisů společnosti.

Z hlediska vnitřní implementace by šlo o změnu registrací těchto zařízení. Díky tomuto zásahu by nebylo nutné nijak upravovat technologii ANC, která je na tento způsob přiřazování přichystána.

3.3 Návrh řešení třetí hypotézy

V předchozí hypotéze bylo navrženo opatření, které zabrání možnosti se do virtuální sítě připojit a mít možnosti ji napadnout. Pro případ, že by byla objevena nová zranitelnost je důležité zajistit, aby k ARP poisoning útok a další podobné útoky nemohly nastat.

Nejlepší obranou proti podobným typům útoků je aktivní analýza a filtrování packetů. Tato technika spoléhá na analýzu všech packetů procházející sítí a v případě nalezení podezřele se chovajících packetů je dokáže zablokovat. V momentě , kdy se jedná o útok v rámci lokální sítě, dokáže útočníka zablokovat a nedovolit v pokračování útoku. Existuje několik možných způsobů, jak tento problém řešit. Jedno z možných řešení je dokoupit specializované zařízení, které se bude starat výlučně o filtraci sítě, druhá možnost je nastavit filtrování na serveru a poslední možnost je nejvhodnější, a to nastavit filtrování a na firewallu.

V současné chvíli z hlediska finančního i rychlosti nasazení je nejlepší možnost změnit konfiguraci na firewallech. To ovšem přináší překážku, jelikož takto rozsáhlá změna konfigurace vyžaduje znovu nastavení celého zařízení. Pro možnost tuto rekonfiguraci zařídit u firewallu od firmy Clavister je nutné, aby byl součástí hlavní softwarově podporované větve. Tedy zařízení s podporou Clavister cOS, což jsou z hlediska podporovaných zařízení ze strany klienta Clavister E80, W30 a W40.

V současné době je na celém světě v provozu odhadem 3 400 center, která je potřeba ochránit. V případě 2 100 z těchto center, na kterých je jich nainstalován aktuální hardware není nutné pořizovat nové zařízení a bude se jednat pouze o softwarovou aktualizaci a rekonfiguraci. V případě zbylých 1 300 centrech bude nutné zařízení vyměnit za nové modely, které jsou schopny splnit potřebné podmínky.

Při výpočtu nákladů na tuto změnu bude brána v potaz cena pouze zařízení Clavister E80, jelikož je to zařízení s dostatečnou propustností. Pouze ve výjimečných případech jsou nasazována zařízení s vyšším výkonem. Cena tohoto zařízení je 350 liber a poplatek

za instalaci a konfiguraci firewallu se rovná 250 librám. V součtu tedy 600 liber na každé centrum s nevyhovujícím hardwarem.

Po nainstalování a aktualizování nových i stávajících zařízení je nutné zajistit nové měření a penetrační testování a tím se ujistit, že aplikovaná opatření fungují efektivně, a především je schopno útokům zabránit.

3.4 Ekonomické zhodnocení

Tato kapitola se věnuje ekonomickému zhodnocení celé práce. Nejdříve vyčíslí ekonomickou náročnost pro uskutečnění jednotlivých hypotéz a nutnost jejich provedení. Poté bude v poslední kapitole shrnuta celková finanční náročnost opatření a případná finanční rizika, která by mohla ovlivnit fungování společnosti.

3.4.1 Hypotéza jedna

Hypotéza jedna v současné chvíli nepředstavuje bezpečnostní hrozbu z hlediska zkoumané hypotézy, náklady na vyřešení objeveného problému, ale budou započítány do finálního výsledku. A to z důvodu nebezpečí způsobeného provozováním zastaralých přepínačů a případným dalším nebezpečím spojených s chybami, které se během přiřazování vyskytují.

V současném momentě je na celém světě asi 3 400 aktivních center z nichž dvě třetiny má v provozu aspoň jeden nepodporovaný přepínač. Podle reportu aktivních zařízení vychází na každé centrum s nepodporovaným hardware asi 1,73 přepínačů. Tento počet bude využit pro výpočet nákladů na náhradu těch nepodporovaných. Cena za instalaci nového zařízení je 250 liber a cena nového zařízení je 600 liber. Cena za instalaci nového zařízení bude započítána podle počtu center, ve kterých jsou nainstalované nepodporované přepínače, jelikož instalace je účtována jako paušál a je možné během ní nainstalovat více zařízení najednou.

Tabulka 14: Investice na výměnu zastaralých přepínačů.

	Počty center a zařízení	Náklady na výměnu
Počet dotčených center	2 250 center	562 500 liber
Počet dotřených zařízení	3 892 zařízení	2 335 200 liber
Součet		2 897 700 liber

3.4.2 Hypotéza dvě

V případě hypotézy dvě není nutné pro aktuálně vybrané řešení investovat žádné finance pro aplikování navrhnutých změn. Jediné, co bude nutné do této změny investovat, bude čas vývojového týmu společnosti.

3.4.3 Hypotéza tři

Třetí hypotéza představuje vážnou bezpečnostní hrozbu v případě prolomení ochrany virtuální sítě. O tento problém se jedná všech 3 400 center, výhodou je že 2 100 z nich bude stačit pouze aktualizovat a rekonfigurovat software na již fungujících firewallech. Tento úkon může být uskutečněn během údržby bez přítomnosti technika na místě. Je tu sice riziko výpadku internetu v případě neúspěšné aktualizace, ale jelikož se podobné úkony dělají běžně za provozu, tohle riziko je akceptovatelné. Zbylých 1 300 center bude vyžadovat aktualizaci jak softwaru, tak hardwaru. Nákup nového zařízení stojí 350 liber a výjezd technika kvůli jeho instalaci dalších 250 liber. Celkové náklady pro instalaci jednoho zařízení je tedy 600 liber.

Tabulka 15: Investice na výměnu zastaralých firewallů.

	Počty center a zařízení	Náklady na výměnu
Počet dotčených center	1 300 center	780 000 liber

3.4.4 Souhrnné zhodnocení

Podle současných zákonů, které jsou platné ve Velké Británií, která je v této práci brána jako příklad pro pokuty za ztráty dat, se pokuta může vyšplhat až na 17,5 milionu liber. Tyto pokuty jsou podobné i v celé Evropské Unii, jsou postupně zaváděny po celém světě. Z tohoto důvodu je důležité opatření aplikovat plošně pro celou firmu, a ne pouze

v dotyčných zemích. Navíc v případě aplikování projektu najednou se snižují náklady díky jednotnému projektovému řízení a tím i snížením časových nákladů managementu.

Pro potřeby této práce budou brány v potaz pokuty ve výši 10 milionů liber za bezpečnostní incident, protože se pokuty nejvyšší možné výše v podstatě nevyskytují a nedávají.

Tabulka 16: Výše celkové investice do řešení bezpečnosti.

	Výše investice
Investice na vyřešení hypotézy jedna	2 897 700 liber
Investice na vyřešení hypotézy dvě	780 000 liber
Celková investice	3 677 700 liber

V současné době je instalovaná investice poměrně nová a k pokusům o prolomení zřejmě ještě nedošlo. To ovšem neznamená, že se tak nestane. V případě bezpečnosti z pravidla platí, že investice do prevence je nižší než případné kompenzace, které plynou z následných pokut a podobných komplikací. Tohle pravidlo se potvrzuje i teď.

V situaci, kdy proběhl úspěšný útok a vytvořil bezpečnostní incident je pokuta, kterou tato práce používá 10 mil. liber. Pokud by se podařilo útok provést, odškodnění může považovat každý poškozený klient a to znamená, že se potenciální finanční škoda může vyšplhat k hodnotě v desítkách milionech liber. Tabulka 17 ukazuje, že i v případě jediného incidentu, do kterého bude zapojen pouze jeden klient, se finanční škoda vyšplhá na trojnásobek nutné investice pro zlepšení fungování tohoto systému.

Tabulka 17: Porovnání nákladů a potenciální pokuty.

Investice pro lepší zabezpečení		Pokuta za ztrátu dat klienta
3 677 700 liber	<	10 000 000 liber

Závěr

Cíle práce, které byly pro tuto práci vytvořeny na základě skutečné zkušenosti se systémem ANC, který je v této práci rozebírán, testován a popisován byly splněny. Během testování vytvořených hypotéz se prokázala jejich úplná nebo částečná pravdivost.

V případě první hypotézy, která se prokázala pouze částečně, se objevily chyby v přidělování VLAN, které sice v současné chvíli neohrožují systém jako takový ze strany bezpečnosti, ale jsou nepříjemné pro zákazníky a mohou snižovat jejich spokojenost. Navíc v případě, kdy v systému existuje jakákoli nekonzistentnost může se nakonec objevit i bezpečnostní trhlina ohrožující systém jako celek. . Z tohoto důvodu je doporučeno co nejdříve aktualizovat software zařízení a poté začít s hromadnou výměnou zařízení, která tyto chyby způsobuje. Finanční náklady na výměnu těchto zařízení jsou 2 897 700 liber.

Druhá hypotéza potvrzuje perfektní funkčnost technologie ANC při používání podporovaného hardware a software. Prokazuje ovšem i bezpečnostní díru v systému přiřazování VLAN a možnosti napadení VLAN klienta. Dále navrhuje systém vícefázového ověření (MFA), který by tento problém vyřešil, jelikož by ověřoval provázanost zařízení s klientem pro zařízení s operačním systémem a pro ostatní navrhuje systém kombinující statické IP adresy a jejich vyjmutí rozsahu pro DHCP. Navržený systém, který počítá s napojením na již fungující robustní informační systém společnosti bude vyvíjen vývojovým oddělením společnosti. Z toho důvodu budou náklady na vývoj nulové. Nevýhodou tohoto řešení je delší doba vývoje z důvodu vzniku několika paralelních projektů v jednu chvíli. Velkou výhodou je ovšem možnost aplikování změn v průběhu vyvíjení s větší flexibilitou, než by byla schopna externí vývojová společnost.

Hypotéza tři se také prokázala. Objevila v systému zásadní bezpečnostní problém. Tento problém je způsoben špatně navrženou ochranou jednotlivých virtuálních sítí. Návrh tohoto řešení počítá s rekonfigurací zařízení, které jsou dost moderní, aby je bylo možné využít pro hloubkovou analýzu packetů v rámci všech sítí na centru. Zařízení, která již nejsou schopny tuto funkci vykonávat musí být vyměněny za nové. V tomto případě se jedná o nová zařízení za 780 000 liber, tato částka zahrnuje i fyzickou instalaci.

V průběhu instalací by měly probíhat i rekonfigurace ostatních podporovaných zařízení pro zajištění co nejrychlejší a nejlepší ochrany.

Z hlediska ekonomického zhodnocení projektu jde o srovnání potenciální pokuty, která může být společnosti vyměřena za únik klientských dat. Ta může dosáhnout až do výše 10 000 000 liber. Z tohoto důvodu je cena 3 677 700 liber za zabezpečení sítě přijatelná. V případě úniku dat je navíc velká pravděpodobnost, že dojde ke ztrátě dat více společností a každá z nich bude moct žádat odškodnění. V takové fázi se konečná finanční škoda může vyšplhat na desítky milionů liber.

SEZNAM POUŽITÝCH ZDROJŮ

1. *Počítačové sítě - přednáška.* **ONDRÁK, V.** Brno : autor neznámý, 2014. VUT v Brně, Fakulta podnikatelská.

2. **JORDÁN, V a ONDRÁK, V.** *Infrastruktura komunikačních systémů I: Univerzální kabelážní systémy.* Brno : CERM, Akademické nakladatelství, 2015. Sv. 2. vyd. ISBN 978-80-214-5115-5.

3. **DONAHUE, G. A.** *Kompletní průvodce síťového experta.* Brno : Computer Press, 2009. Sv. Vyd. 1. ISBN 978-80-251-2247-1.

4. **KUROSE, J, ROSS, K a JONÁK, J.** *Počítačové sítě.* Brno : Computer Press, 2014. Sv. 1. vyd. ISBN 978-80-251-3825-0.

5. **Cisco.** What Is Network Automation? *Cisco.* [Online] [Citace: 09. 05 2021.] https://www.cisco.com/c/en/us/solutions/automation/network-automation.html.

6. **BOUŠKA, P.** Cisco IOS 3 - nastavení interface/portu - access, trunk, port security. [Online] 18. 05 2009. [Citace: 09. 04 2021.] https://www.samuraj-cz.com/clanek/cisco-ios-3-nastaveni-interfaceportu-access-trunk-port-security/.

7. **Cisco.com.** Understanding VLAN Trunk Protocol (VTP). [Online] 29. 09 2014. [Citace: 10. 04 2021.] https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html.

8. **BOUŠKA, P.** VLAN - Virtual Local Area Network. [Online] 02. 06 2007. [Citace: 07. 04 2021.] https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/.

9. **KERCHEVAL, B.** *DHCP: A Guide to Dynamic TCP/IP Network Configuration.* Hoboken : Prentice Hall, 1998. ISBN: 978-0130997210.

10. **KRČMÁŘ, P.** *Linux - tipy a triky pro bezpečnost.* Praha : Grada Publishing, 2004. ISBN 80-247-0812-4.

11. **JORDÁN, V a ONDRÁK, V.** *Infrastruktura komunikačních systémů III: Integrovaná podniková infrastruktura.* Brno : CERM, Akademické nakladatelství, 2015. Sv. 1. vyd. ISBN 978-80-214-5241-1.

12. **DOUCEK, P, KONEČNÝ, M a NOVÁK, L.** *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Praha : Professional publishing, 2019. ISBN 978-80-88260-39-4.

13. **MCKEOWN, E.** What Is Multi-factor Authentication (MFA)? [Online] PingIdentity, 03. 09 2020. [Citace: 18. 04 2021.] https://www.pingidentity.com/en/company/blog/posts/2017/what-is-multi-factor-authentication-mfa.html.

14. **SELECKÝ, M.** *Penetrační testy a exploitace.* Brno : Computer Press, 2012. ISBN 978-80-251-3752-9.

15. **JORDÁN, V a ONDRÁK, V.** *Infrastruktura komunikačních systémů II: Kritické aplikace.* Brno : CERM, Akademické nakladatelství, 2015. Sv. 1. vyd. ISBN 978-80-214-5240-4.

16. **FADYUSHIN, V a HYSLOP, B.** *Instant penetration testing: Setting up a test lab how-to.* Birmingham : Packt Publishing, 2013. ISBN 978-1-84969-412-4.

17. **HARRIS, S.** *Hacking: manuál hackera.* Praha : Grada, 2008. Sv. 1. vyd. ISBN 978-80-247-1346-5.

18. **DROMS, R.** Dynamic Host Configuration Protocol. *Network Working Group.* [Online] 03 1997. [Citace: 07. 04 2021.] https://www.rfc-editor.org/rfc/rfc2131.txt.

19. **POSTILL, D.** Understanding DHCP discovery specific subnet. [Online] 14. 09 2014. [Citace: 07. 04 2021.] https://superuser.com/questions/811501/understanding-dhcp-discovery-specific-subnet.

20. **ZURČÁK, M.** Bezpečnosť na LAN pod lupou: DHCP spoofing. [Online] 11. 08 2011. [Citace: 07. 04 2021.] https://secit.sk/sk/content/bezpecnost-na-lan-pod-lupou-dhcp-spoofing.

21. **HOWARD.** What Is DHCP Snooping and How It Works? [Online] 07. 10 2019. [Citace: 07. 04 2021.] https://community.fs.com/blog/what-is-dhcp-snooping-and-how-it-works.html.

22. **ZURČÁK, M.** Bezpečnosť na LAN pod lupou: Úvod a útok ARP cache poisoning. [Online] 05. 07 2011. [Citace: 07. 04 2021.] https://secit.sk/sk/content/bezpecnost-na-lan-pod-lupou-uvod-utok-arp-cache-poisoning.

23. **SPANGLER, R.** Packet sniffing on layer 2 switched local area networks. [Online] 2003. [Citace: 07. 04 2021.] http://www.packetwatch.net/documents/papers/layer2sniffing.pdf.

24. **VEJVODOVA, J.** We deliver IT services, products and solutions. [Online] [Citace: 15. 04 2021.] https://dworkin.eu/.

25. **Interní informace společnosti. London : autor neznámý, 2021.**

26. SHI, Ch. and YU, P. S. ***Heterogeneous Information Network Analysis and Applications.*** **Cham : Springer International Publishing, 2017. ISBN: 978-3-319-56212-4.**

27. Kali Docs. [Online] OffSec Services Limited. [Citace: 20. 04 2021.] https://www.kali.org/docs/.

28. Wireshark docs. [Online] [Citace: 20. 04 2021.] https://www.wireshark.org/docs/.

29. ORNAGHI, A. a VEALLERI, M. ABOUT THE ETTERCAP PROJECT. [Online] Ettercap Project. [Citace: 20. 04 2021.] https://www.ettercap-project.org/about.html.

30. Corp, Famatech. Advanced IP Scanner - About Us. [Online] [Citace: 27. 04 2021.] https://www.advanced-ip-scanner.com/about/.

31. Putty. [Online] [Citace: 02. 05 2021.] https://www.putty.org/.

32. Penalties. [Online] [Citace: 15. 04 2021.] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/penalties/.

Seznam použitých obrázků

Seznam použitých tabulek

Seznam použitých grafů

Abecední seznam zkratek

ANC – Automated Network Configuration

AP – Access Point

CIO – Chief Information Officer

DHCP – Dynamic Host Configuration Protocol

IEEE – Institute of Electrical and Electronics Engineers

IMS – Integrated Management System (Integrovaný systém řízení)

IP – Internet Protocol

LAN – Local Area Network

MAN – Metropolian Arena Network

MiTM – Man in The Middle

NAS – Network Attached Storage

VLAN – Virtuální síť

WAN – Wide Arena Network

WS – (Workstation) je označení obecné pracovní stanice v síti

Přílohy

Příloha I: Analýza Zefis

Příloha II: Měření – hypotéza jedna

Příloha III: Měření – hypotéza dvě